



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出 願 年 月 日

Date of Application:

2002年 2月19日

出 願 番 号

Application Number:

特願2002-041890

ST.10/C]:

[JP2002-041890]

出 願 人

Applicant(s):

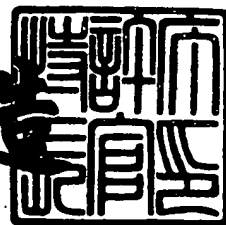
株式会社ソニー・コンピュータエンタテインメント

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 3月 8日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2002-3014529

u3

【書類名】 特許願
【整理番号】 SCEI01206
【あて先】 特許庁長官殿
【国際特許分類】 G06K 1/00
G06N 1/00

【発明者】

【住所又は居所】 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コン
ピュータエンタテインメント内

【氏名】 島田 宗毅

【発明者】

【住所又は居所】 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コン
ピュータエンタテインメント内

【氏名】 岡本 伸一

【発明者】

【住所又は居所】 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コン
ピュータエンタテインメント内

【氏名】 吉森 正治

【発明者】

【住所又は居所】 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コン
ピュータエンタテインメント内

【氏名】 犬井 努

【発明者】

【住所又は居所】 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コン
ピュータエンタテインメント内

【氏名】 島川 恵三

【発明者】

【住所又は居所】 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コン
ピュータエンタテインメント内

【氏名】 岡田 豊史

【発明者】

【住所又は居所】 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 九保 亮

【発明者】

【住所又は居所】 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 中村 光宏

【特許出願人】

【識別番号】 395015319

【氏名又は名称】 株式会社ソニー・コンピュータエンタテインメント

【代理人】

【識別番号】 100107238

【弁理士】

【氏名又は名称】 米山 尚志

【先の出願に基づく優先権主張】

【出願番号】 特願2001- 44358

【出願日】 平成13年 2月20日

【手数料の表示】

【予納台帳番号】 111236

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0014358

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コピー管理システム、クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、クライアント端末装置の情報処理プログラム、管理サーバ装置の情報処理プログラム、コピー管理方法、クライアント端末装置の情報処理方法、及び管理サーバ装置の情報処理方法

【特許請求の範囲】

【請求項 1】 暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付され、管理者側からユーザに配布される記憶媒体と、

上記記憶媒体に記憶されているコンテンツを、上記暗号化鍵に対応する復号化鍵を用いて復号化して二次記憶媒体にコピーするコピー機能を有し、該コンテンツのコピーを行う際に、上記記憶媒体の媒体識別情報と共に、所定かつ固有のデバイス識別情報を送信するユーザの端末装置と、

上記記憶媒体の媒体識別番号を受信した際に、上記デバイス識別情報を有するユーザの端末装置に対して、上記コンテンツの復号化鍵を送信する管理サーバ装置と

を有するコピー管理システム。

【請求項 2】 請求項 1 記載のコピー管理システムであって、

上記管理サーバ装置は、一つの媒体識別情報に対して 1 回のみ復号化鍵の送信を行うこと

を特徴とするコピー管理システム。

【請求項 3】 請求項 1 又は請求項 2 記載のコピー管理システムであって、

上記端末装置は、上記端末装置の識別情報、上記コンテンツのコピーを行うコピー手段に固有に付された識別情報、及び外付けの半導体メモリに固有に付された識別番号のうち、いずれか 1 つ或いは複数を組み合わせ、上記デバイス識別情報として送信すること

を特徴とするコピー管理システム。

【請求項 4】 請求項 1 から請求項 3 のうち、いずれか一項記載のコピー管

理システムであって、

上記管理サーバ装置は、上記デバイス識別情報で上記復号化鍵を暗号化して送信し、

上記端末装置は、自己のデバイス識別情報で、上記暗号化された復号化鍵を復号化して用いること

を特徴とするコピー管理システム。

【請求項 5】 請求項 1 から請求項 4 のうち、いずれか一項記載のコピー管理システムであって、

上記端末装置は、上記コンテンツの復号化後に、上記復号化鍵を削除すること
を特徴とするコピー管理システム。

【請求項 6】 請求項 1 から請求項 5 のうち、いずれか一項記載のコピー管理システムであって、

上記管理サーバ装置は、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信し、

上記端末装置は、上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーし、上記再暗号化鍵を記憶手段に記憶し、上記記憶手段に記憶した再暗号化鍵を用いて、上記コピーされたコンテンツを復号化して再生すること

を特徴とするコピー管理システム。

【請求項 7】 請求項 1 から請求項 6 のうち、いずれか一項記載のコピー管理システムであって、

上記管理サーバ装置は、各ユーザのデバイス識別情報に関連付けして上記復号化鍵を送信済みの媒体識別情報をデータベースに記憶することで上記復号化鍵の配信管理を行い、修理或いは交換によりユーザのデバイス識別情報が変更された場合、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えること

を特徴とするコピー管理システム。

【請求項 8】 請求項 1 から請求項 7 のうち、いずれか一項記載のコピー管理システムであって、

上記管理サーバ装置は、復号化鍵の送信を行った端末装置を有するユーザに対して所定の課金処理を行うこと

を特徴とするコピー管理システム。

【請求項 9】 請求項 1 から請求項 8 のうち、いずれか一項記載のコピー管理システムであって、

上記ユーザの端末装置と上記管理サーバ装置との間で情報の送受信を仲介すると共に、少なくとも上記復号化鍵をユーザの端末装置に送信した際に、ユーザに対する課金処理を行う仲介サーバ装置を有すること

を特徴とするコピー管理システム。

【請求項 10】 暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、

ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出すステップと、

少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信するステップと、

上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信するステップと、

上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理するステップと、

上記復号化処理したコンテンツをコピーするステップと

を有するクライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 11】 請求項 10 記載の記憶媒体であって、

上記復号化鍵を受信するステップは、ユーザのデバイスのデバイス識別情報で暗号化されて送信される復号化鍵を受信し、

上記コンテンツを復号化処理するステップは、自己のデバイスのデバイス識別情報で、上記暗号化されている復号化鍵を復号化処理し、この復号化処理した復号化鍵を用いて上記記憶媒体に記憶されているコンテンツを復号化処理すること

を特徴とする記憶媒体。

【請求項 1 2】 請求項 1 0 又は請求項 1 1 記載の記憶媒体であって、
上記コンテンツのコピー後に、上記復号化鍵を削除するステップを有すること
を特徴とする記憶媒体。

【請求項 1 3】 請求項 1 0 から請求項 1 2 のうち、いずれか一項記載の記憶媒体であって、

上記管理サーバ装置から送信される、上記コピーするコンテンツを再暗号化するための再暗号化鍵を受信するステップと、

上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーするステップと、

上記再暗号化鍵を記憶手段に記憶するステップと、

コンテンツを再生する際に、上記記憶手段に記憶されている再暗号化鍵を用いて上記コピーされたコンテンツを復号化して再生するステップと

を有することを特徴とする記憶媒体。

【請求項 1 4】 請求項 1 0 から請求項 1 3 のうち、いずれか一項記載の記憶媒体であって、

上記媒体識別情報及びデバイス識別情報を送信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を送信すること

を特徴とする記憶媒体。

【請求項 1 5】 ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、

各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出するステップと、

上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信するステップと
を有する管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 1 6】 請求項 1 5 記載の記憶媒体であって、

上記復号化鍵の送信を行った媒体識別情報を、該送信を行ったユーザのデバイスのデバイス識別番号に関連付けて上記データベースに登録するステップを有すること
を特徴とする記憶媒体。

【請求項 1 7】 請求項 1 5 又は請求項 1 6 記載の記憶媒体であって、

上記復号化鍵を送信するステップは、ユーザのデバイスのデバイス識別情報で、上記復号化鍵を暗号化して送信すること
を特徴とする記憶媒体。

【請求項 1 8】 請求項 1 5 から請求項 1 7 のうち、いずれか一項記載の記憶媒体であって、

上記復号化鍵を送信するステップは、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信すること
を特徴とする記憶媒体。

【請求項 1 9】 請求項 1 5 から請求項 1 8 のうち、いずれか一項記載の記憶媒体であって、

修理或いは交換によりユーザのデバイスに対して新たなデバイス識別情報が付与された際に、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えるステップを有すること

を特徴とする記憶媒体。

【請求項 2 0】 請求項 1 5 から請求項 1 9 のうち、いずれか一項記載の記憶媒体であって、

上記復号化鍵の送信を行ったユーザに対して課金を行うステップを有すること
を特徴とする記憶媒体。

【請求項 2 1】 請求項 1 5 から請求項 2 0 のうち、いずれか一項記載の記

載の記憶媒体であって、

上記媒体識別情報及びデバイス識別情報受信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を受信することを特徴とする記憶媒体。

【請求項 2 2】 暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、

ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出すステップと、

少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信するステップと、

上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信するステップと、

上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化处理するステップと、

上記復号化处理したコンテンツをコピーするステップと

を有するクライアント端末装置の情報処理プログラム。

【請求項 2 3】 請求項 2 2 記載の情報処理プログラムであって、

上記復号化鍵を受信するステップは、ユーザのデバイスのデバイス識別情報で暗号化されて送信される復号化鍵を受信し、

上記コンテンツを復号化处理するステップは、自己のデバイスのデバイス識別情報で、上記暗号化されている復号化鍵を復号化处理し、この復号化处理した復号化鍵を用いて上記記憶媒体に記憶されているコンテンツを復号化处理することを特徴とする情報処理プログラム。

【請求項 2 4】 請求項 2 2 又は請求項 2 3 記載の情報処理プログラムであって、

上記コンテンツのコピー後に、上記復号化鍵を削除するステップを有すること
を特徴とする情報処理プログラム。

【請求項 2 5】 請求項 2 2 から請求項 2 4 のうち、いずれか一項記載の情報処理プログラムであって、

上記管理サーバ装置から送信される、上記コピーするコンテンツを再暗号化するための再暗号化鍵を受信するステップと、

上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーするステップと、

上記再暗号化鍵を記憶手段に記憶するステップと、

コンテンツを再生する際に、上記記憶手段に記憶されている再暗号化鍵を用いて上記コピーされたコンテンツを復号化して再生するステップと

を有することを特徴とする情報処理プログラム。

【請求項 2 6】 請求項 2 2 から請求項 2 5 のうち、いずれか一項記載の情報処理プログラムであって、

上記媒体識別情報及びデバイス識別情報を送信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を送信すること

を特徴とする情報処理プログラム。

【請求項 2 7】 ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、

各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出するステップと、

上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信するステップと

を有する管理サーバ装置の情報処理プログラム。

【請求項 2 8】 請求項 2 7 記載の情報処理プログラムであって、

上記復号化鍵の送信を行った媒体識別情報を、該送信を行ったユーザのデバイスのデバイス識別番号に関連付けて上記データベースに登録するステップを有すること

を特徴とする情報処理プログラム。

【請求項 2 9】 請求項 2 7 又は請求項 2 8 記載の情報処理プログラムであって、

上記復号化鍵を送信するステップは、ユーザのデバイスのデバイス識別情報で、上記復号化鍵を暗号化して送信すること

を特徴とする情報処理プログラム。

【請求項 3 0】 請求項 2 7 から請求項 2 9 のうち、いずれか一項記載の情報処理プログラムであって、

上記復号化鍵を送信するステップは、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信すること

を特徴とする情報処理プログラム。

【請求項 3 1】 請求項 2 7 から請求項 3 0 のうち、いずれか一項記載の情報処理プログラムであって、

修理或いは交換によりユーザのデバイスに対して新たなデバイス識別情報が付与された際に、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えるステップを有すること

を特徴とする情報処理プログラム。

【請求項 3 2】 請求項 2 7 から請求項 3 1 のうち、いずれか一項記載の情報処理プログラムであって、

上記復号化鍵の送信を行ったユーザに対して課金を行うステップを有することを特徴とする情報処理プログラム。

【請求項 3 3】 請求項 2 7 から請求項 3 2 のうち、いずれか一項記載の記載の情報処理プログラムであって、

上記媒体識別情報及びデバイス識別情報受信するステップでは、該デバイス識

別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を受信することを特徴とする情報処理プログラム。

【請求項 3 4】 固有のデバイス識別番号が付されたユーザのデバイスで、固有の媒体識別情報が付された記憶媒体に暗号化鍵で暗号化されて記憶されているコンテンツのコピーを行う際に、上記デバイスから上記デバイス識別情報及び上記媒体識別情報を管理サーバ装置に送信し、

コンテンツのコピーが行われた記憶媒体の媒体識別情報が、各ユーザのデバイスのデバイス識別情報に関連付けされた状態で登録されるデータベースに、上記ユーザのデバイスから送信された媒体識別情報が登録されているか否かを上記管理サーバ装置が検出し、

上記データベースに、上記媒体識別情報が未登録であった場合に、上記管理サーバ装置からユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信する

コピー管理方法。

【請求項 3 5】 暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出し、

ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出し、

少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信し、

上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信し、

上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理し、

上記復号化処理したコンテンツをコピーする

クライアント端末装置の情報処理方法。

【請求項 3 6】 ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信し、

各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出し、

上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信する

管理サーバ装置の情報処理方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、例えばゲームコンテンツ、映画コンテンツ、音楽コンテンツ、アプリケーションプログラム等のコンピュータプログラムのコピー管理を行うコピー管理システム、クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、クライアント端末装置の情報処理プログラム、管理サーバ装置の情報処理プログラム、コピー管理方法、クライアント端末装置の情報処理方法、及び管理サーバ装置の情報処理方法に関する。

【0 0 0 2】

【従来の技術】

今日において、例えばCD-ROM、DVD-ROM或いは半導体メモリ等の記憶媒体に記憶されているゲームコンテンツに基づいてビデオゲームを実行するビデオゲーム機が広く普及している。

【0 0 0 3】

ユーザは、所望のゲームコンテンツが記憶された記憶媒体を購入し、この記憶媒体をビデオゲーム機で再生してビデオゲームを行う。大抵の場合、ユーザは、徐々に新しいビデオゲームを買い揃えていく。このため、月日と共にユーザの手元には各ゲームコンテンツが記憶された記憶媒体が蓄積されていくこととなる。

【0004】

しかし、ビデオゲーム機には、記憶媒体の再生機構が1基のみ設けられている場合が多い。このため、異なるビデオゲームを行う場合には、ビデオゲーム機に現在装着されている記憶媒体を取り出し、これから行おうとするゲームコンテンツが記憶された記憶媒体を新たに装着し直すという、大変面倒な作業を必要としていた。

【0005】

【発明が解決しようとする課題】

本件出願人は、例えば数十G（ギガ）オーダーの大容量のハードディスクドライブ（HDD）を内蔵或いは外付け可能としたビデオゲーム機を開示している。

【0006】

このビデオゲーム機の場合、各記憶媒体に記憶されているゲームコンテンツをそれぞれHDDにコピーし、このHDDから所望のゲームコンテンツを再生して利用することができる。このHDDを用いることにより、ビデオゲーム機の再生機構に記憶媒体を着脱する手間を省略することができる。

【0007】

ここで、ゲームコンテンツ等のコンピュータプログラムは、そのコンピュータプログラムが記憶されたソフトウェアを購入する等して正当に入手したユーザのみが使用可能なはずである。

【0008】

しかし、記憶媒体に記憶されたコンピュータプログラムを二次記憶媒体にコピー可能とした場合、一つの記憶媒体に記憶されているコンピュータプログラムを、複数のユーザがそれぞれ二次記憶媒体にコピーして使用する不正コピーが懸念される。

【0009】

本発明は、上述の課題に鑑みてなされたものであり、正当なユーザに対してのみ、コンピュータプログラムのコピーを可能とするコピー管理を行うことで、コンテンツの不正使用の防止等を図ったコピー管理システム、クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、管

理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、クライアント端末装置の情報処理プログラム、管理サーバ装置の情報処理プログラム、コピー管理方法、クライアント端末装置の情報処理方法、及び管理サーバ装置の情報処理方法の提供を目的とする。

【 0 0 1 0 】

【課題を解決するための手段】

本発明は、暗号化鍵で暗号化したコンテンツを記憶させた記憶媒体に対して固有の識別番号を付してユーザに配布する。ユーザがコンテンツのコピーを行う際に使用するデバイスにも識別番号が付されている。

【 0 0 1 1 】

上記デバイスは、コンテンツのコピーを行う際に、上記記憶媒体の識別番号、及びデバイスの識別番号を管理サーバ装置に送信する。管理サーバ装置は、各ユーザが使用するデバイスの識別番号が登録されたデータベースを有している。管理サーバ装置は、データベースに登録されているデバイスの識別番号と、ユーザのデバイスから送信されたデバイスの識別番号とを照合してユーザを特定する。管理サーバ装置は、この照合を行うことでユーザが特定された際に、記憶媒体に記憶されているコンテンツを復号化するための復号化鍵をユーザのデバイスに送信する。

【 0 0 1 2 】

ユーザのデバイスは、この管理者側から配布された復号化鍵に基づいて上記記憶媒体に記憶されているコンテンツを復号化してコンテンツのコピーを行う。

【 0 0 1 3 】

これにより、記憶媒体の持ち主である正規のユーザにのみ、コンテンツのコピーを許可することができ、コンテンツの不正コピーを防止することができる。

【 0 0 1 4 】

【発明の実施の形態】

本発明は、コンピュータプログラムのコピー管理を行うコピー管理システムに適用することができる。

【 0 0 1 5 】

コンピュータプログラムとしては、例えばゲームコンテンツ、音楽コンテンツ、映画コンテンツ、アプリケーションプログラム等がある。また、コンピュータプログラムが記憶された記憶媒体としては、DVD-ROM、CD-ROM等の光ディスクの他、半導体メモリがある。また、コンピュータプログラムのコピー先となる二次記憶媒体としては、ハードディスク（HD）、DVD-RAMや光磁気ディスク（MO）等がある。

【0016】

以下、上記ゲームコンテンツ、音楽コンテンツ、映画コンテンツ、アプリケーションプログラム等を総称して、単に「コンテンツ」ということとする。

【0017】

〔コピー管理システムの全体構成〕

まず、図1に本発明の第1の実施の形態となるコピー管理システムの全体構成を示す。この図1に示すように、この第1の実施の形態のコピー管理システムは、光ディスクに記憶されているコンテンツの再生機能（実行機能）、及びネットワークを介した通信機能を備えたクライアント端末装置1を有している。

【0018】

このクライアント端末装置1には、光ディスクに記憶されたコンテンツをコピーするためのハードディスクドライブ2（HDD）が接続されている。

【0019】

また、このクライアント端末装置1には、インターネット5などのネットワークとの接続を図るための通信モデム6が接続されている。

【0020】

なお、通信モデム6は、この図1に示すようにクライアント端末装置1に対して外付けのかたちで設けてもよい。また、通信モデム6は、クライアント端末装置1に内蔵のかたちで設けてもよい。

【0021】

また、コピー管理システムは、ユーザエントリ情報が記憶されたデータベース3を備えたシステムサーバ装置4を有している。

【0022】

このシステムサーバ装置 4 と上記クライアント端末装置 1 とが、例えばインターネット 5 等のネットワークを介して相互に接続されることでこの第 1 の実施の形態のコピー管理システムが構成されている。

【 0 0 2 3 】

〔クライアント端末装置の構成〕

図 2 に、クライアント端末装置 1 の外観の斜視図を示す。この図 2 示すように、クライアント端末装置 1 の前面側には、コントローラ接続部 7 A、7 B と、メモリカード装着部 8 A、8 B が設けられている。

【 0 0 2 4 】

また、このクライアント端末装置 1 の前面側には、USB 対応機器 (USB : Universal Serial Bus) が接続される 2 つの USB 接続端子 9 と、例えば最大 4 0 0 M b p s のデータ転送速度に対応可能な IEEE 1 3 9 4 接続端子 1 0 とが設けられている。

【 0 0 2 5 】

また、このクライアント端末装置 1 の前面側には、光ディスクが装着されるトレイ型のディスク装着部 1 1 が設けられている。

【 0 0 2 6 】

また、このクライアント端末装置 1 の前面側には、コンテンツの実行動作や再生動作をリセットするためのリセットボタン 1 2 と、光ディスク装着部 1 1 のトレイの出し入れを操作するためのトレイ操作ボタン 1 3 とが設けられている。

【 0 0 2 7 】

クライアント端末装置 1 の背面側には、電源スイッチ、音声映像出力端子 (A V マルチ出力端子)、P C カードスロット、光デジタル出力端子、A C 電源入力端子等が設けられている。

【 0 0 2 8 】

A V マルチ出力端子は、A V ケーブル 1 7 を介してモニタ用のテレビジョン受像機 1 8 に接続される。クライアント端末装置 1 から出力される映像信号や音声信号は、この A V マルチ出力端子及び A V ケーブル 1 7 を介してモニタ用のテレビジョン受像機 1 8 に供給される。これにより、上記コンテンツの映像がテレビ

ジョン受像機 1 8 に表示される。また、上記コンテンツの音声がテレビジョン受像機のスピーカ装置を介して発音される。

【 0 0 2 9 】

コントローラ接続部 7 A、7 B には、コントローラケーブル 1 5 を介してそれぞれコントローラ 1 4 が接続される。

【 0 0 3 0 】

メモ리카ード装着部 8 A、8 B には、ゲームデータのセーブ（記憶）及び読み出しを行うセーブ用のメモ리카ード等が装着される。

【 0 0 3 1 】

〔ハードディスクドライブの構成〕

次に、図 2 において、クライアント端末装置 1 の上面部に載置されている筐体がハードディスクドライブ 2（以下、HDD 2 という）である。この HDD 2 は、内部に例えば 4 0 G B 等の大容量のハードディスクが設けられている。この HDD 2 には、十数枚分の DVD-ROM に記憶されたゲームコンテンツをコピー可能となっている。

【 0 0 3 2 】

HDD 2 の前面側には、電源投入時に点灯駆動される電源ランプ 2 0 と、ハードディスクへの書き込みに連動して点灯駆動される書き込み表示ランプ 2 1 とが設けられている。HDD 2 の背面側には、少なくとも電源スイッチ及びデータ入出力端子が設けられている。

【 0 0 3 3 】

HDD 2 をクライアント端末装置 1 に接続する場合、クライアント端末装置 1 の背面側に設けられた上記 PC カードスロットに PC カードを挿入する。この状態で、PC カードに接続ケーブルの一端を接続する。接続ケーブルの他端は、HDD 2 のデータ入出力端子に接続する。これにより、クライアント端末装置 1 と HDD 2 とが、電氣的に相互に接続される。

【 0 0 3 4 】

なお、この例においては、HDD 2 はクライアント端末装置 1 とは別体で、クライアント端末装置 1 に対して外付けすることとした。しかし、この HDD 2 を

、クライアント端末装置 1 に内蔵するかたちで設けてもよい。

【0035】

また、クライアント端末装置 1 と HDD 2 とを PC カードと接続ケーブルを介して接続することとした。しかし、HDD 2 の背面側（或いは前面側でもよい。）に USB 接続端子や IEEE 1394 接続端子等の接続端子を設け、この接続端子を介して HDD 2 をクライアント端末装置 1 に接続するようにしてもよい。

【0036】

〔クライアント端末装置の電氣的構成〕

次に、図 3 はクライアント端末装置 1 のブロック図である。この図 3 に示すように、クライアント端末装置 1 は、CPU 30 と、グラフィックプロセッサ 31（GPU）と、IO プロセッサ 32（IOP）を有している。

【0037】

また、クライアント端末装置 1 は、CD-ROM や DVD-ROM 等の光ディスクの再生制御を行う光ディスク制御部 33 と、サウンドプロセッサユニット 34（SPU）とを有している。

【0038】

また、クライアント端末装置 1 は、CPU 30 や IOP 32 が実行するオペレーティングシステムプログラムが格納された MASK-ROM 35 と、CPU 30 のワークエリアや光ディスクから読み出されたデータを一時的に格納するバッファとして機能する RAM 36 とを有している。

【0039】

また、クライアント端末装置 1 は、光ディスク制御部 33 の RF アンプ 37 を介して供給される光ディスクからの再生出力に対して、例えば誤り訂正処理（CRC 処理）等を施して出力する CD/DVDDSP 38 を有している。

【0040】

また、クライアント端末装置 1 は、光ディスク制御部 33 のスピンドルモータの回転制御、光ピックアップのフォーカス／トラッキング制御、ディスクトレイのローディング制御等を行うドライバ 39 及びメカコントローラ 40 を有している。

【 0 0 4 1 】

また、クライアント端末装置 1 は、上記 P C カードが接続されるカード型コネクタ 4 1 を有している。

【 0 0 4 2 】

これらの各部は、主にバスライン 4 2, 4 3 等を介してそれぞれ相互に接続されている。

【 0 0 4 3 】

なお、DVD-ROM に記憶された映画コンテンツの再生は、メモリカードに記憶された DVD ドライバソフトウェアに基づいて行われる。或いは、映画コンテンツの再生は、クライアント端末装置 1 内に内蔵された半導体メモリ 4 4 (DVD Player ROM) に焼き付けられた DVD ドライバソフトウェアに基づいて行われる。

【 0 0 4 4 】

MASK-ROM 3 5 には、オペレーティングシステムプログラムが記憶されている。CPU 3 0 は、この MASK-ROM 3 5 に記憶されているオペレーティングシステムプログラムに基づいて、クライアント端末装置 1 全体の動作を制御する。

【 0 0 4 5 】

また、MASK-ROM 3 5 には、コントローラ接続部 7 A, 7 B と、メモリカード装着部 8 A, 8 B、及びカード型コネクタ 4 1 に接続されるコントローラ 1 4, メモリカード 1 6 及び HDD 2 等のハードウェア識別番号 (ハードウェア ID) も記憶されている。IOP 3 2 は、この MASK-ROM 3 5 に記憶されているハードウェア ID に基づいて、コントローラ 1 4, メモリカード 1 6 及び HDD 2 等のハードウェアと通信を行い、各接続端子 7 A, 7 B, 8 A, 8 B 及びカード型コネクタ 4 1 等に接続されたハードウェアを特定して認識する。

【 0 0 4 6 】

なお、ハードウェア ID は、クライアント端末装置 1 全体で一つの ID、メモリカード 1 6 全体で一つの ID、及び HDD 2 全体で一つの ID 等のように、いわば各ハードウェアに対して総称的に付された ID を意味している。

【 0 0 4 7 】

これに対して、後述するクライアントID、MC-ID及びHDD-IDは、各クライアント端末装置1毎、各メモ리카ード16毎、及び各HDD2毎にそれぞれ付された各ハードウェア固有のIDとなっている。

【 0 0 4 8 】

GPU31は、CPU30からの描画指示に従って描画を行い、描画された画像を図示しないフレームバッファに格納する。また、GPU31は、座標変換等の処理を行うジオメトリトランスファエンジンとしての機能を有している。

【 0 0 4 9 】

このGPU31は、例えば光ディスクに記録されているゲームコンテンツがいわゆる3Dグラフィックを利用する場合に、三角形状のポリゴンの集合で仮想的な3次元オブジェクトを構成する。そして、GPU31は、この3次元オブジェクトを仮想的なカメラ装置で撮影することで得られる画像を生成するための諸計算を行う。すなわち、GPU31は、レンダリングを行う場合における透視変換処理（3次元オブジェクトを構成する各ポリゴンの頂点を仮想的なカメラスクリーン上に投影した場合における座標値の計算）等を行う。

【 0 0 5 0 】

また、GPU31は、CPU30からの描画指示に従って、必要に応じてジオメトリトランスファエンジンを利用しながら、フレームバッファに対して描画を行う。そして、この描画した画像に対応するビデオ信号（visual out）を出力する。

【 0 0 5 1 】

一方、SPU34は、適応予測符号化された音声データを再生するADPCM復号機能と、サウンドバッファに記憶されている波形データを再生することで、効果音等の音声信号を再生して出力（audio out）する再生機能と、サウンドバッファに記憶されている波形データを変調させて再生する変調機能等を備えている。このSPU34は、いわゆるサンプリング音源として動作する。SPU34は、CPU30からの指示により、サウンドバッファに記憶されている波形データに基づき楽音、効果音等の音声信号を発生する。

【 0 0 5 2 】

このようなクライアント端末装置 1 は、電源が投入されると、CPU 3 0 及び IOP 3 2 が、MASK-ROM 3 5 から CPU 3 0 用のオペレーティングシステムプログラム及び IOP 3 2 用のオペレーティングシステムプログラムをそれぞれ読み出す。

【 0 0 5 3 】

CPU 3 0 は、CPU 3 0 用のオペレーティングシステムプログラムによりクライアント端末装置 1 の各部を統括的に制御する。

IOP 3 2 は、IOP 3 2 用のオペレーティングシステムプログラムによりコントローラ 1 4、メモリカード 1 6、及び HDD 2 等との間のデータの入出力を制御する。

【 0 0 5 4 】

CPU 3 0 は、CPU 3 0 用のオペレーティングシステムプログラムに基づいて、動作確認等の初期化処理を行った後、光ディスク制御部 3 3 を制御し、光ディスクに記録されているコンテンツを再生制御する。

【 0 0 5 5 】

再生したコンテンツがビデオゲームのゲームコンテンツである場合、CPU 3 0 は、IOP 3 2 を介してコントローラ 1 4 から受け付けたプレーヤからの指示（コマンド）に従って、GPU 3 1 や SPU 3 4 を制御し、ゲームコンテンツの画像の表示や効果音、楽音等の発声を制御する。

【 0 0 5 6 】

再生したコンテンツが映画コンテンツの場合、CPU 3 0 は、IOP 3 2 を介してコントローラ 1 4 から受け付けたプレーヤからの指示に従って、GPU 3 1 や SPU 3 4 を制御し、映画コンテンツの映像の表示や音声の発声等を制御する。

【 0 0 5 7 】

〔コピー管理動作〕

このようなコピー管理システムは、光ディスクに記憶されているコンテンツが HDD 2 にコピーされる際に、以下のように管理する。

【0058】

〔インストーラのインストール〕

まず、このコピー管理システムは、光ディスクに記憶されているコンテンツをHDD2にコピーする際に、クライアント端末装置1でコピー制御用のアプリケーションプログラム（インストーラ）を実行する必要がある。この例の場合、インストーラは、コンテンツと共に光ディスクに記憶されている。クライアント端末装置1は、コンテンツのコピーを行う前にインストーラのインストールを行う。

【0059】

インストーラのインストールを行う場合、ユーザは、インストーラが記憶されている光ディスクをクライアント端末装置1に装着する。クライアント端末装置1のCPU30は、この光ディスクが装着されると自動的に（オートラン）、或いはユーザのコントローラ14の操作に従って光ディスクに記憶されているインストーラを読み出し、これをメモリカード16或いはRAM36に記憶制御する。

【0060】

このメモリカード16或いはRAM36に記憶されたインストーラは、ユーザが光ディスクに記憶されているコンテンツのコピーを指定した際に、CPU30により実行される。CPU30は、このインストーラを実行することで、コンテンツのコピー制御を行う。

【0061】

なお、インストーラは、システム業者側でインストーラのみ記憶された光ディスクを製造し、これをユーザに配布するようにしてもよい。
或いは、システム業者側でインストーラが記憶されたメモリカードを製造し、これをユーザに配布するようにしてもよい。この場合、インストーラのインストール作業を省略可能とすることができる。

【0062】

或いは、インストーラが記憶されたROMをクライアント端末装置1内に設けてもよい。この場合でも、インストーラのインストール作業を省略可能とすることができる。

【 0 0 6 3 】

〔コンテンツの暗号化〕

光ディスクに記憶されたコンテンツには、図 4 に示すように各コンテンツ毎に異なる対称鍵（コンテンツキー：Content-Key）を用いて暗号化処理が施されている。また、光ディスクには、このように暗号化処理されたコンテンツの他、各光ディスク毎に固有となる「Media unique ID（メディアユニーク ID：MID）」が記憶されている。

【 0 0 6 4 】

〔ユーザ登録〕

次に、この第 1 の実施の形態のコピー管理システムにおいては、光ディスクから HDD 2 にコンテンツのコピーを行う場合、各メモ리카ード 1 6 に固有に付された「メモ리카ード ID（MC-ID）」を用いてシステムサーバ装置 4 にユーザ登録を行う。このユーザ登録が行われない場合には、コンテンツのコピーは許可されない。

【 0 0 6 5 】

図 5 は、ユーザがシステムサーバ装置 4 に対してユーザ登録を行うまでの流れを示すフローチャートである。図 6 は、このユーザ登録によりクライアント端末装置 1 とシステムサーバ装置 4 との間で送受信される情報を示す当該コピー管理システムの模式図である。

【 0 0 6 6 】

この図 5 及び図 6 を用いてユーザ登録動作を説明する。図 5 のフローチャートは、ユーザがクライアント端末装置 1 のメイン電源を投入することでスタートとなる。

【 0 0 6 7 】

ステップ S 1 では、ユーザがインターネット 5 を介して自分のクライアント端末装置 1 をシステムサーバ装置 4 に接続する。

【 0 0 6 8 】

具体的には、このクライアント端末装置 1 には、図 1 に示したようにインターネット接続用の通信モデム 6 が接続（或いは内蔵）されている。ユーザによりイ

インターネット接続が指定されると、図3に示すCPU30は、所定のWWWブラウザに基づいて動作し、この通信モデム6を介して当該クライアント端末装置1とシステムサーバ装置4との間の通信回線の確立を図る。これにより、このユーザ登録の行程がステップS2に進む。

【0069】

ステップS2では、CPU30が、クライアント端末装置1に装着されたメモリカードの識別番号(MC-ID)、クライアント端末装置1毎に付された固有の識別番号(クライアントID)及びHDD2毎に付された固有の識別番号(HDD-ID)をシステムサーバ装置4に送信制御する。

【0070】

具体的には、システムサーバ装置4とクライアント端末装置1との通信回線が確立されると、CPU30は、クライアント端末装置1、HDD2及びメモリカード16とそれぞれ通信を行う。CPU30は、この通信により、クライアント端末装置1に固有に付された識別番号(クライアントID)、HDD2に固有に付された識別番号(HDD-ID)、及びクライアント端末装置1に装着されたメモリカード16に固有に付された識別番号(MC-ID)をそれぞれ取得する。

【0071】

CPU30は、これらの識別番号を、図6に示すようにシステムサーバ装置4側に送信する。これにより、このユーザ登録の行程がステップS3に進む。

【0072】

なお、クライアント端末装置1とシステムサーバ装置4との間においては、例えばSSL(Secure Sockets Layer)等の通信プロトコルに基づいて情報が暗号化されて送受信されるようになっており、通信の安全性が確保されている。

【0073】

また、この例においては、CPU30は、各デバイスと通信を行うことで、クライアントID、HDD-ID及びMC-IDを取得してシステムサーバ装置4側に送信することとした。しかし、クライアント端末装置1、HDD2及びメモリカード16には、クライアントID、HDD-ID及びMC-IDがそれぞれ

各筐体にユーザが視認可能なかたちで貼り付けられている。このため、ユーザが、このクライアントID、HDD-ID及びMC-IDを見て、コントローラ14を操作して手動で各IDの入力を行い、システムサーバ装置4側に送信するようにしてもよい。

【0074】

次に、ステップS3では、システムサーバ装置4が、このユーザから送信されたメモリカードの識別番号(MC-ID)が有効なIDであるか否かを判別する。このユーザ登録行程は、このステップS3において、システムサーバ装置4が、ユーザから送信されたMC-IDが有効なIDであると判別した場合にステップS4に進み、ユーザから送信されたMC-IDが無効なIDであると判別した場合にステップS7に進む。

【0075】

具体的には、システムサーバ装置4は、全てのクライアント端末装置1のクライアントID、全てのHDD2のHDD-ID、及び全てのメモリカード16のMC-IDを記憶したデータベース3を有している。

【0076】

システムサーバ装置4は、ユーザからクライアント端末装置1、HDD2及びメモリカード16の各固有のIDが送信されると、まず、ユーザから送信されたメモリカード16の固有のIDであるMC-IDと、データベース3に登録されている各MC-IDとを照合し、ユーザから送信されたメモリカード16のMC-IDと同じMC-IDがデータベース3に登録されているか否かを判別する。

【0077】

すなわち、システムサーバ装置4は、ユーザから送信されたメモリカード16のMC-IDは、データベース3に正規に登録されているMC-IDと同じであるか否かを判別する。

【0078】

ユーザから送信されたメモリカード16のMC-IDが、データベース3に正規に登録されているいずれのMC-IDとも一致しなかった場合には、システムサーバ装置4は、このユーザ登録のアクセスを、不正なユーザ登録のアクセスと

判断する。この場合、システムサーバ装置4は、ステップS7において、例えば「このメモリカードではユーザ登録を行うことはできません。」等のユーザ登録を拒否するメッセージをクライアント端末装置1側に返信する（無効通知）。これにより、ユーザ登録が中断されたかたちで、このユーザ登録行程が終了することとなる。

【0079】

一方、ユーザから送信されたメモリカード16のMC-IDが、データベース3に正規に登録されているいずれかのMC-IDと一致した場合、システムサーバ装置4は、ステップS4において、現在、システムサーバ装置4にアクセスしているユーザの固有のIDであるユーザID（User ID）を、例えば乱数等を用いて形成する。

【0080】

そして、システムサーバ装置4は、図6に示すようにそのユーザのクライアントID、HDD-ID及びMC-IDと共に、上記ユーザの固有のIDであるユーザID（User ID）、及び後に説明するMC-Keyを一纏めにし、これを「ユーザエントリ情報」としてシステムサーバ装置4のデータベース3に登録する。

【0081】

このように、当該実施の形態のコピー管理システムは、各ユーザが所有するクライアント端末装置1、HDD2及びメモリカード16の3つのIDの組み合わせで各ユーザを特定してデータベース3に登録する。

【0082】

クライアント端末装置1、HDD2及びメモリカード16の3つのIDが、異なるユーザ間で全て一致するということは有り得ないため、この3つのIDに基づいてユーザ登録を行うことにより、ユーザを確実に特定してユーザ登録を行うことができる。これにより、後述する光ディスクに記録されたコンテンツの不正コピーを、より強力に防止することができる。

【0083】

なお、ユーザ登録の際に、「MC-IDのみ」、「クライアントIDのみ」、

「HDD-IDのみ」、「MC-IDとクライアントID」、「MC-IDとHDD-ID」、或いは「クライアントIDとHDD-ID」をシステムサーバ装置4側に送信してユーザ登録を行うようにしてもよい。これらの場合でも、各IDはそれぞれ固有のIDであるため、異なるユーザ間で重複することはなく、ユーザを略々確実に特定してユーザ登録を行うことができる。

【0084】

次に、ユーザ登録の行程がステップS5に進むと、システムサーバ装置4は、ユーザ登録が正規に完了した証として、上記ステップS4で形成したユーザエントリ情報のうち、ユーザID (User ID) をMC-Keyで暗号化し、これをクライアント端末装置1側に返信する。

【0085】

[MC-Key]

ここで、上記「MC-Key」は、クライアント端末装置1とシステムサーバ装置4との間で送受信する情報を暗号化するための鍵情報である。このMC-Keyは、MC-IDと共にメモリカード16内に予め記憶されている。

【0086】

MC-IDは、ユーザが視認可能なようにメモリカード16の筐体に張り付けられているのであるが、このMC-Keyはユーザが視認できないようにメモリカード16内に記憶されている。また、このMC-Keyは、ユーザがメモリカード16内に記憶されている情報を再生した場合でも、表示や出力が行われることのない秘密性の高い情報となっている。このため、このMC-Keyは、ユーザレベルでは、認識することはできないようになっている。

【0087】

また、システムサーバ装置4のデータベース3には、全てのメモリカード16のMC-IDと共に、各メモリカード16に記憶されたMC-Keyが記憶されている。システムサーバ装置4は、MC-Keyが必要となったときに、このデータベース3からMC-Keyを読み出して参照する。このため、クライアント端末装置1からシステムサーバ装置4に対してMC-Keyが送信されることはない。

【0088】

このように、MC-Keyは、ユーザレベルでは認識することができず、また、クライアント端末装置1とシステムサーバ装置4との間で送受信されることの無い、秘密性の高い情報となっている。

【0089】

クライアント端末装置1とシステムサーバ装置4との間におけるMC-Keyの送受信を不要とすることで、MC-Keyが第三者に傍受される不都合を防止することができる。

【0090】

システムサーバ装置4は、ユーザID (User ID) を返信する際、予めデータベース3に記憶されているMC-Keyの中から、現在アクセスされているユーザのメモリカード16に対応するMC-Keyを選択する。そして、この選択したMC-Keyを用いてユーザID (User ID) を暗号化してクライアント端末装置1に返信する。

【0091】

このMC-Keyは、上記ユーザID (User ID) , メディアユニークID (media unique ID (MID)) , コンテンツキー (Content-Key) 、及びContent-Gen-Keyをそれぞれ復号化する際に用いられる。

【0092】

MIDは、各光ディスク毎に固有に付されているIDである。コンテンツキーは、光ディスクに記録されたコンテンツを暗号化処理する際に用いられた暗号鍵である。Content-Gen-Keyは、HDD2にコピーされるコンテンツに対して再暗号化処理を施す際に用いられる暗号鍵である。

【0093】

クライアント端末装置1は、光ディスクから再生したコンテンツを、上記コンテンツキーを用いて復号化する。そして、クライアント端末装置1は、この復号化したコンテンツを、上記Content-Gen-Keyを用いて再暗号化処理してHDD2にコピーするようになっている。詳しくは後述する。

【0094】

次に、ユーザ登録行程がステップS6に進むと、クライアント端末装置1が、システムサーバ装置4側から返信されたユーザID (User ID) をメモリカード16に記憶制御する。これにより、この図5のフローチャートに示すユーザ登録の全行程が終了する。そして、この時点において、メモリカード16には、図6に示すように予め記憶されているMC-ID及びMC-Keyと共に、MC-Keyで暗号化されたユーザID (User ID) が記憶されることとなる。

【0095】

〔メディアユニークIDの登録とコンテンツキーの取得〕

次に、光ディスクに記録されているコンテンツを何回でもHDD2にコピー可能とすると、MC-ID、MC-Key及びユーザID (User ID) が記録されたメモリカード16を他のユーザに貸与するだけで、この他のユーザも光ディスクに記録されているコンテンツをこの他のユーザのHDDに不正にコピーすることが可能となり好ましいことではない。

【0096】

このコピー管理システムの場合、コンテンツをHDD2にコピーする際、ユーザがクライアント端末装置1を介して各光ディスク毎に付された固有のメディアユニークID (media unique ID (MID)) をシステムサーバ装置4側に送信する。システムサーバ装置4は、ユーザから送信されたメディアユニークIDを登録すると共に、暗号化されたコンテンツを復号化するためのコンテンツキーをユーザに送信する。クライアント端末装置1は、光ディスクに記録されているコンテンツを、コンテンツキーを用いて復号化してHDD2にコピーする。このため、このコンテンツキーを受信するということは、システムサーバ装置4からクライアント端末装置1に対して、コンテンツのコピーが許諾されたことを意味する。

【0097】

システムサーバ装置4は、クライアント端末装置1から受信したメディアユニークIDに対して、過去にコンテンツキーの送信が行われていないことを確認し

たうえで、コンテンツキーの送信を行う。これにより、同じメディアユニーク ID に対するコンテンツキーの送信を、1 回のみに制限することができる。

【0098】

例えば、あるユーザが自分で購入した光ディスクに記憶されているコンテンツを、自分の HDD 2 にコピーした後に、この光ディスクを他のユーザに貸与したとする。他のユーザは、HDD 2 にコンテンツをコピーする際に、貸与された光ディスクのメディアユニーク ID をシステムサーバ装置 4 に送信する。

【0099】

しかし、システムサーバ装置 4 側には、その光ディスクのメディアユニーク ID に対して、コンテンツキーの送信が行われたことを示す履歴が残っている。この場合、システムサーバ装置 4 は、他のユーザに対してコンテンツキーの配信は行わない。コンテンツキーを入手することができない他のユーザは、コンテンツを HDD 2 にコピーすることはできない。このコピー管理システムは、このようにしてコンテンツの不正コピーを防止している。

【0100】

図 7 のフローチャートに、メディアユニーク ID (MID) の登録とユーザがコンテンツキーを取得するまでの流れを示す。また、図 8 に、メディアユニーク ID の登録の際、及びコンテンツキーの取得の際に、クライアント端末装置 1 とシステムサーバ装置 4 との間で送受信される各情報を示す。

【0101】

この図 7 及び図 8 を用いてメディアユニーク ID (MID) の登録とコンテンツキーの取得動作を説明する。この図 7 のフローチャートに示すメディアユニーク ID (MID) の登録とコンテンツキーの取得行程（登録取得行程）は、ユーザが前述のユーザ登録を正規に終了させていることを前提として実行される。

【0102】

まず、ステップ S 1 1 では、クライアント端末装置 1 が、システムサーバ装置 4 との間の通信回線の確立を図る。これにより、この登録取得行程がステップ S 1 2 に進む。

【0103】

なお、この例においては、前述のユーザ登録終了後に、クライアント端末装置 1 とシステムサーバ装置 4 との間で確立された通信回線を一旦切断し、この登録取得行程の実行時に、再度、クライアント端末装置 1 とシステムサーバ装置 4 との間の通信回線を確立する説明となっている。

【 0 1 0 4 】

しかし、前述のユーザ登録に続けて、クライアント端末装置 1 とシステムサーバ装置 4 との間で確立された通信回線を切断することなく、この登録取得行程を実行するようにしてもよい。この場合、この登録取得行程は、ステップ S 1 1 をスキップして、スタートからステップ S 1 2 に進むこととなる。

【 0 1 0 5 】

次にステップ S 1 2 では、クライアント端末装置 1 が、前述のように取得したユーザ ID (U s e r I D) 及び MC - I D をシステムサーバ装置 4 に送信する。また、クライアント端末装置 1 は、このユーザ ID 及び MC - I D と共に、これから HDD 2 にコピーするコンテンツが記憶された光ディスクに対して固有に付されているメディアユニーク ID (M I D) をシステムサーバ装置 4 側に送信する。

【 0 1 0 6 】

具体的には、CPU 3 0 は、メモリカード 1 6 と通信を行い、図 8 に示すように MC - I D をシステムサーバ装置 4 側に送信する。また、CPU 3 0 は、前述のように MC - K e y で暗号化されたユーザ ID をメモリカード 1 6 から読み出してシステムサーバ装置 4 側に送信する。また、CPU 3 0 は、光ディスク制御部 3 3 を制御して光ディスクから再生したメディアユニーク ID (M I D) を MC - K e y で暗号化し、これをシステムサーバ装置 4 側に送信する。

【 0 1 0 7 】

なお、これらの各情報と共に、クライアント ID 及び HDD - I D をシステムサーバ装置 4 側に送信するようにしてもよい。クライアント ID 及び HDD - I D は、上記 MC - I D と共にユーザの特定に用いることができる。MC - I D , クライアント ID 及び HDD - I D の 3 つの ID を用いてユーザを特定することで、MC - I D のみでユーザの特定を行う場合よりも、より正確にユーザを特定

することができる。

【0108】

また、クライアント端末装置1とシステムサーバ装置4との間で送受信される情報は、例えばSSL (Secure Sockets Layer) 等の通信プロトコルに基づいて暗号化されて送受信される。これにより、クライアント端末装置1とシステムサーバ装置4との間では、安全性の高い通信を行うことができる。

【0109】

次に、ステップS13では、システムサーバ装置4が、クライアント端末装置1側から送信されたユーザID (User ID) が有効なIDであるか否かを判別する。このステップS13において、システムサーバ装置4が、ユーザIDは有効であると判別した場合、この登録取得行程がステップS14に進む。これに対して、このステップS13において、システムサーバ装置4が、ユーザIDは無効であると判別した場合、この登録取得行程はステップS17に進む。

【0110】

具体的には、システムサーバ装置4は、クライアント端末装置1側から送信されたMC-ID (及びクライアントID, HDD-ID) に基づいてデータベース3を参照し、このMC-IDに対応するMC-Keyを読み出す。そして、システムサーバ装置4は、このMC-Keyに基づいて、MC-Keyで暗号化されて送信されたユーザID (User ID) 及びメディアユニークID (MID) をそれぞれ復号化する。

【0111】

前述のように、システムサーバ装置4側のデータベース3には、ユーザエントリ情報としてユーザID (User ID), MC-ID, クライアントID及びHDD-ID等が記憶されている。このため、システムサーバ装置4は、MC-ID (クライアントID及びHDD-ID) に基づいてデータベース3内のユーザ情報を検索する。そして、システムサーバ装置4は、このユーザ情報内のユーザID (User ID) と、現在システムサーバ装置4側にアクセスしてきているユーザのユーザID (User ID) とを照合する。

システムサーバ装置4は、上記両者が一致した場合には、現在システムサーバ装

置4側にアクセスしてきているユーザは正規のユーザであると判断する。これにより、この登録取得行程がステップS14に進む。

【0112】

これに対して、システムサーバ装置4は、データベース3のユーザ情報内のユーザID (User ID) と、現在システムサーバ装置4側にアクセスしてきているユーザのユーザID (User ID) とが不一致の場合、そのユーザID (User ID) は無効と判断する。そして、システムサーバ装置4は、ステップS17において、例えば「ユーザIDが無効です。ユーザ登録をして下さい。」等の再度のユーザ登録を促すメッセージをクライアント端末装置1側に返信する(無効通知)。これにより、この登録取得行程が中断されたかたちで終了することとなる。

【0113】

次に、ステップS14では、システムサーバ装置4が、現在アクセスしてきているユーザの光ディスクに記録されているコンテンツは、過去にコピーされた履歴があるか否かを判別する。

【0114】

具体的には、このコピー管理システムの場合、データベース3に、各光ディスクにそれぞれ付されているメディアユニークID (MID) が全て登録されている。システムサーバ装置4は、コンテンツのコピーが行われた際に、データベース3のメディアユニークID (MID) に対してフラグを立てることで、コピーの履歴を残すようになっている。

【0115】

このため、システムサーバ装置4は、メディアユニークID (MID) を復号化すると、そのメディアユニークID (MID) に対してフラグが立っているか否かを検出する。これにより、そのメディアユニークID (MID) を有する光ディスクから過去にコンテンツのコピーが行われたか否かを判別することができる。

【0116】

そのメディアユニークID (MID) のフラグが立っていない場合、そのメデ

メディアユニークID (MID) が付された光ディスクから過去にコンテンツのコピーは行われていないことを意味する。このため、システムサーバ装置4は、データベース3内におけるそのメディアユニークID (MID) のフラグを立てる。また、システムサーバ装置4は、このフラグを立てたメディアユニークID (MID) を、そのユーザのユーザエントリ情報に登録して、この登録取得行程をステップS15に進める。

【0117】

これに対して、そのメディアユニークID (MID) のフラグが立っている場合、過去にそのメディアユニークID (MID) が付された光ディスクからコンテンツのコピーが行われていることを意味する。このため、システムサーバ装置4は、ステップS17において、例えば「このメディアからコンテンツのコピーをすることはできません。」等のコンテンツのコピーを拒否するメッセージをクライアント端末装置1側に返信する（無効通知）。これにより、この登録取得行程が中断されたかたちで終了することとなる。

【0118】

次にステップS15は、過去に、そのユーザの光ディスクからコンテンツのコピーが行われていない場合に進むステップである。この場合、システムサーバ装置4は、そのユーザのメモリカード16のMC-Keyを用いて、光ディスクに記録されているコンテンツを暗号化したコンテンツキー (Content-Key) の暗号化を行う。そして、この暗号化したコンテンツキーをクライアント端末装置1側に送信する。このコンテンツキーの送信は、システムサーバ装置4側からユーザに対して、光ディスクに記録されているコンテンツのコピーが許可されたことを意味する。

【0119】

MC-Keyは、そのユーザが所有するメモリカード16に対して固有に付されている。このため、このコンテンツキーを復号化して使用することができるユーザを、そのMC-Keyが記憶されたメモリカード16を有するユーザのみに限定することができる。従って、上記コンテンツキーを正規のユーザに対してのみ、安全に送信することができる。

【0120】

また、システムサーバ装置4は、データベース3に記憶されているユーザエントリ情報に基づいて、そのユーザが使用しているクライアント端末装置1のクライアントID及びHDD2のHDD-IDを読み出す。システムサーバ装置4は、これら各IDを、例えば乱数を用いて形成した「コンテンツジェンキー (Content-Gen-Key)」で暗号化してクライアント端末装置1側に返信する。

【0121】

さらに、システムサーバ装置4は、クライアントID及びHDD-IDを暗号化する際に用いたコンテンツジェンキー (Content-Gen-Key) を、上記MC-Keyで暗号化してクライアント端末装置1側に返信する。

【0122】

後に説明するが、クライアント端末装置1は、システムサーバ装置4から返信されたクライアントIDと、当該クライアント端末装置1のクライアントIDとを照合する。また、クライアント端末装置1は、システムサーバ装置4から送信されたHDD-IDと、当該クライアント端末装置1に接続されているHDD2のHDD-IDとを照合する。そして、クライアント端末装置1は、上記2つのクライアントIDと、上記2つのHDD-IDとが、それぞれ一致することを確認してコンテンツのコピーを行うようになっている。

【0123】

このため、システムサーバ装置4からユーザのクライアント端末装置1に対して、予め登録されているクライアントID及びHDD-IDを返信することにより、予めデータベース3に登録されているそのユーザのクライアント端末装置1とHDD2の組み合わせでのみ、コンテンツのコピー可能とすることができる。

【0124】

さらに、システムサーバ装置4は、クライアントID及びHDD-IDを暗号化したコンテンツジェンキーを、そのユーザが所有するメモリカード16に固有に付されたMC-Keyを用いて暗号化してユーザのクライアント端末装置1に返信する。これにより、コンテンツジェンキーを復号化して使用することができ

るユーザを、そのMC-Keyが記憶されたメモリカード16を有するユーザのみに限定することができる。従って、上記コンテンツジェンキーを正規のユーザに対してのみ、安全に送信することができる。

【0125】

次に、ステップS16では、クライアント端末装置1が、システムサーバ装置4側から返信されたMC-Keyで暗号化されたコンテンツキー(Content-Key)、MC-Keyで暗号化されたコンテンツジェンキー(Content-Gen-Key)、及びコンテンツジェンキー(Content-Gen-Key)で暗号化されたクライアントID及びHDD-IDをそれぞれメモリカード16に記憶制御する。これにより、この図7のフローチャートに示す登録取得行程が終了する。

【0126】

このように、このコピー管理システムは、過去にコピー履歴の無いメディアユニークID(MID)を有する光ディスクに記憶されたコンテンツのみコピーの許可を行う。これにより、各光ディスクに記憶されたコンテンツのコピーを1回に制限することができる。このため、過去にコンテンツのコピーが行われた光ディスクを貸与された第三者は、その貸与された光ディスクからコンテンツのコピーを行うことはできない。従って、1枚の光ディスクから多数のユーザがコンテンツのコピーを行う不正使用を防止することができる。

【0127】

〔コンテンツのコピー〕

次に、ユーザは、このコンテンツキー(Content-Key)を取得することで、光ディスクに記録されているコンテンツをHDD2にコピーすることが可能となる。

【0128】

図9はこのコピー行程の流れを示すフローチャート、図10はこのコンテンツのコピーが行われる際に、クライアント端末装置1、HDD2及びメモリカード16の間で取り扱う情報を模式的に示した図である。この図9及び図10を用いてコンテンツのコピー行程の説明を行う。

【 0 1 2 9 】

まず、図 9 のフローチャートは、前述のメディアユニーク ID の登録を終了し、コンテンツキーを取得したユーザが、クライアント端末装置 1 を操作してコンテンツのコピーを指定することでスタートとなる。

【 0 1 3 0 】

ステップ S 2 1 では、クライアント端末装置 1 の I O P 3 2 が、それぞれ MC - K e y で暗号化されたコンテンツキー (C o n t e n t - K e y) 及びコンテンツジェンキー (C o n t e n t - G e n - K e y) をメモリカード 1 6 から読み出し、これらを C P U 3 0 に供給する。

【 0 1 3 1 】

前述のように、MC - K e y は、システムサーバ装置 4 及びこのクライアント端末装置 1 でそれぞれ保持している。このため、C P U 3 0 は、この保持している MC - K e y を用いて、上記暗号化されているコンテンツキー (C o n t e n t - K e y) 及びコンテンツジェンキー (C o n t e n t - G e n - K e y) を復号化処理する。そして、C P U 3 0 は、この復号化したコンテンツキー及びコンテンツジェンキーを R A M 3 6 に記憶制御する。これにより、このコピー行程がステップ S 2 2 に進む。

【 0 1 3 2 】

ステップ S 2 2 では、I O P 3 2 が、コンテンツジェンキー (C o n t e n t - G e n - K e y) で暗号化されたクライアント ID 及び HDD - I D をメモリカード 1 6 から読み出し、これらを C P U 3 0 に供給する。C P U 3 0 は、先に復号化したコンテンツジェンキー (C o n t e n t - G e n - K e y) を用いてこのクライアント ID 及び HDD - I D を復号化する。

【 0 1 3 3 】

また、このステップ S 2 2 では、C P U 3 0 が、上記復号化したクライアント ID と当該クライアント端末装置 1 に付されたクライアント ID とを照合する。また、C P U 3 0 は、上記復号化した HDD - I D と、当該クライアント端末装置 1 に接続された HDD 2 の HDD - I D とを照合する。

【 0 1 3 4 】

次に、ステップ S 2 3 では、CPU 3 0 が、上記各クライアント ID、及び上記各 HDD - ID がそれぞれ一致するか否かを判別する。両者が一致する場合はコンテンツのコピーを実行すべくこのコピー行程がステップ S 2 4 に進む。両者が不一致の場合はこのコピー行程がステップ S 2 8 に進む。

【 0 1 3 5 】

メモ리카ード 1 6 から復号化されたクライアント ID 及び HDD - ID が、そのクライアント端末装置 1 のクライアント ID 及び HDD - ID と一致しないということは、前述のコンテンツキー (Content - Key) の取得が、正規のユーザのクライアント端末装置 1 及び HDD 2 に基づいて行われていないことを示す。

【 0 1 3 6 】

すなわち、この場合、正規ユーザからメモ리카ード 1 6 を貸与された不正ユーザが、コンテンツのコピーを行おうとしていることを示している。

【 0 1 3 7 】

このため、CPU 3 0 は、例えば「コピーを行うことはできません。」等のコンテンツのコピーを拒否するメッセージをユーザに対して表示制御する。これにより、中断されたかたちでこのコピー行程が終了することとなる。

【 0 1 3 8 】

次に、ステップ S 2 4 は、クライアント端末装置 1 が、上記各クライアント ID 及び上記各 HDD - ID の一致を検出した際に実行するステップである。この場合、CPU 3 0 は、光ディスク制御部 3 3 により光ディスクから再生されたコンテンツを、RAM 3 6 に記憶されているコンテンツキー (Content - Key) を用いて復号化する。また、CPU 3 0 は、この復号化したコンテンツを、RAM 3 6 に記憶されているコンテンツジェンキー (Content - Gen - Key) で再暗号化して HDD 2 に供給する。

【 0 1 3 9 】

次に、ステップ S 2 5 では、HDD 2 が、図 1 0 に示すように上記コンテンツジェンキーで再暗号化されたコンテンツをハードディスクに保存 (コピー) する。

【 0 1 4 0 】

次に、ステップ S 2 6 ではクライアント端末装置 1 の CPU 3 0 が HDD 2 と通信を行うことで、コンテンツのコピーが完了したか否かを判別する。コピーが完了していない場合、CPU 3 0 は、前述のステップ S 2 4 及びステップ S 2 5 の動作を繰り返し実行制御することで、コンテンツのコピーが完了するまでの間、HDD 2 に対してコンテンツの供給を行う。コンテンツのコピーが完了すると、このコピー行程がステップ S 2 7 に進む。

【 0 1 4 1 】

ステップ S 2 7 では、コンテンツのコピーが完了したため、IOP 3 2 が、メモリカード 1 6 に記憶されているコンテンツキー (Content-Key) を消去する。これにより、このコピー行程が終了する。

【 0 1 4 2 】

このように、クライアント端末装置 1 は、コンテンツキー (Content-Key) で暗号化されて光ディスクに記憶されているコンテンツを、システムサーバ装置 4 から発行されたコンテンツキーで復号化して HDD 2 にコピーする。そして、このコンテンツのコピー後に、メモリカード 1 6 内に記憶されているコンテンツキー (システムサーバ装置 4 から発行されたコンテンツキー) を消去する。

【 0 1 4 3 】

前述のように、過去にコンテンツのコピーが行われた光ディスクに対しては、データベース 3 にコピー履歴が残るため、システムサーバ装置 4 は、原則的にコンテンツキーの再発行は行わない。このため、一度コンテンツのコピーが行われた光ディスクを貸与された第三者からのコピー申請は、システムサーバ装置 4 が、上記データベースのコピー履歴に基づいて拒否する。そして、システムサーバ装置 4 は、この第三者に対しては、コンテンツキーを送信しない。

【 0 1 4 4 】

上記第三者は、コンテンツキーを取得することができないため、貸与された光ディスクに記憶されているコンテンツを復号化することができない。このため、上記第三者がコンテンツを HDD 等の二次記憶媒体にコピーすることができたと

しても、コンテンツを復号化することができないことから、該コンテンツを使用することができない。従って、このコピー管理システムは、コンテンツの不正使用を防止することができる。

【 0 1 4 5 】

[コピーされたコンテンツの再生]

次に、このようにHDD 2にコピーされたコンテンツは、ユーザが繰り返し再生して利用することができるようになっている。

【 0 1 4 6 】

図 1 1 に、HDD 2 に保存されたコンテンツの再生行程の流れを示すフローチャートを示す。また、図 1 2 にこの再生行程において、クライアント端末装置 1、HDD 2 及びメモ리카ード 1 6 の間で取り扱われる情報の模式図を示す。

【 0 1 4 7 】

図 1 1 のフローチャートは、前述のコンテンツのコピーを正規に終了させたユーザが、コンテンツの再生を指定することでスタートとなる。

【 0 1 4 8 】

ステップ S 3 1 では、クライアント端末装置 1 の I O P 3 2 が、上記MC-Keyで暗号化されたコンテンツジェンキー (Content-Gen-Key) をメモ리카ード 1 6 から読み出し、これをCPU 3 0 に供給する。CPU 3 0 は、このコンテンツジェンキーを、クライアント端末装置 1 側で保持しているMC-Keyを用いて復号化して再生する。

【 0 1 4 9 】

次に、ステップ S 3 2 では、I O P 3 2 が、コンテンツジェンキー (Content-Gen-Key) で暗号化されたクライアントID及びHDD-IDをメモ리카ード 1 6 から読み出し、これをCPU 3 0 に供給する。CPU 3 0 は、先に復号化したコンテンツジェンキーを用いて、この暗号化されたクライアントID及びHDD-IDを復号化する。

【 0 1 5 0 】

次に、ステップ S 3 3 では、CPU 3 0 が、当該クライアント端末装置 1 に付されているクライアントIDと、上記コンテンツジェンキーで復号化したクライ

アントIDとを照合する。

【0151】

また、CPU30は、当該クライアント端末装置1に接続されているHDD2のHDD-IDと、上記コンテンツジェンキーで復号化したHDD-IDとを照合する。

【0152】

上記各クライアントID及び上記各HDD-IDが一致しないということは、他のユーザのメモリカード16、他のユーザのクライアント端末装置1、或いは他のユーザのHDD2が用いられていることを示す。このため、CPU30は、ステップS35において、例えば「コンテンツを再生することはできません。」等のコンテンツの再生を拒否するメッセージをユーザに表示する。これにより、中断されるかたちでこのコンテンツの再生行程が終了することとなる。

【0153】

このように、このコピー管理システムにおいては、HDD2にコピーされたコンテンツを再生する際にも、クライアントID及びHDD-IDの照合を行う。例えば、正規のユーザが所有するメモリカード16とコンテンツが保存されたHDD2が、第三者に貸与された場合を考える。第三者は、自分のクライアント端末装置に対して、この貸与されたメモリカード16とHDD2を接続して、該HDD2内に記憶されているコンテンツの再生を行うこととなる。

【0154】

しかし、メモリカード16内に記憶されているクライアントIDは、正規のユーザのクライアントIDである。このため、第三者のクライアント端末装置のクライアントIDと、メモリカード16に記憶されているクライアントIDとが一致しないことから、第三者のクライアント端末装置において、HDD2に記憶されているコンテンツの再生は拒否される。このため、メモリカード16とHDD2が貸与された場合でも、HDD2にコピーされているコンテンツの使用を防止することができる。

【0155】

次に、上記各クライアントID及び上記各HDD2がそれぞれ一致した場合、

CPU 30は、先に復号化したコンテンツジェンキーを用いてHDD 2のコンテンツを復号化し、これをRAM 36に記憶する。これにより、このコンテンツの再生行程が終了する。

【0156】

RAM 36に記憶されたコンテンツが、例えばビデオゲームのゲームコンテンツであった場合、CPU 30は、このゲームコンテンツに基づいて動作する。そして、CPU 30は、例えばビデオゲームのキャラクタを表示制御し、効果音やBGM等を発音制御する。これにより、ユーザは、光ディスクからHDD 2にコピーしたゲームコンテンツに基づいてビデオゲームを楽しむことができる。

【0157】

光ディスクからゲームコンテンツを直接的に再生してビデオゲームを行う場合、新たなビデオゲームを行う毎に光ディスクの着脱作業が必要である。しかし、このように各光ディスクに記録されたゲームコンテンツをHDD 2にコピーしておくことにより、新たなビデオゲームを行う毎に必要なとなっていた光ディスクの着脱作業を省略することができる。このため、新たなビデオゲームをスムーズに開始可能とすることができる。

【0158】

なお、光ディスクからコンテンツのコピーが終了した後は、メモリカード16に記憶されているコンテンツキーが消去されるため、コンテンツの再コピーは行うことができない。しかし、メモリカード16に記憶されているコンテンツジェンキーは、コピー完了後も消去されることはない。このため、コンテンツジェンキーで暗号化されてHDD 2にコピーされたコンテンツは、このメモリカード16に記憶されているコンテンツジェンキーを用いて繰り返し復号化して再生可能である。

【0159】

[デバイスの修理、交換に対する対応]

次に、このコピー管理システムの場合、システムサーバ装置4は、クライアントID、HDD-ID、MC-ID等（以下、一括してデバイスIDという）と、ユーザIDとをユーザエントリ情報として一括して管理する。しかし、クライ

アント端末装置 1 や HDD 2 等のデバイスを破損等により交換した場合、この交換したデバイスのデバイス ID が、ユーザエントリ情報として登録されているデバイス ID とは異なるものとなる。従って、デバイスの交換を行うと、正規のユーザであるにも拘わらず、その交換したデバイスを用いてコンテンツのコピーや再生が不可能となることが懸念される。

【 0 1 6 0 】

一方、このコピー管理システムの場合、デバイス ID の固有性を確保することでコンテンツの不正使用を防止するようになっている。このため、クライアント端末装置 1 や HDD 2 等のデバイスを修理により復元した場合でも、この修理後のデバイスに対して、修理前に付されていたデバイス ID とは異なる新たなデバイス ID を付し、修理前のデバイスと修理後のデバイスとを明確に区別して管理することが好ましい。

【 0 1 6 1 】

ただ、このように修理後のデバイスに対して新たなデバイス ID を付すと、前述のデバイスの交換時と同様に、正規のユーザであるにも拘わらず、その修理したデバイスを用いてコンテンツのコピーや再生が不可能となることが懸念される。

【 0 1 6 2 】

このコピー管理システムは、デバイスの修理及び交換により新たなデバイス ID を用いることで懸念される上記不都合を、以下のように防止している。

【 0 1 6 3 】

〔クライアント端末装置及び HDD の修理、交換に対する対応〕

図 1 3 に、このコピー管理システムにおけるクライアント端末装置及び HDD の修理、交換に対する対応を説明するための模式図を示す。この図 1 3 中、×印が描かれているクライアント端末装置 1 或いは HDD 2 は、破損したデバイスを示している。

【 0 1 6 4 】

この図 1 3 において、デバイスが破損した場合、ユーザは、その破損したデバイスを、メモリカード 1 6 と共に、このコピー管理システムを管理する管理者側

のリペアセンターに送付する。

【 0 1 6 5 】

すなわち、この場合メモリカード16は破損していないのであるが、メモリカード16にはコンテンツジェンキー (Content-Gen-Key) やコンテンツジェンキー (Content-Gen-Key) で暗号化されたクライアントID及びHDD-ID (以下、各IDを一括してデバイスIDという) が記憶されている。このため、デバイスが破損した場合でも、この破損したデバイスと共にメモリカード16を上記リペアセンターに送付 (或いは持ち込み) するようになっている。

【 0 1 6 6 】

リペアセンターでは、故障したデバイスが送付されると、このデバイスが正常に動作するように修理、交換等すると共に、この修理、交換等したデバイスに対して新たなデバイスIDを付与する。

【 0 1 6 7 】

具体的には、クライアント端末装置1のクライアントIDは、例えば上記ハードウェアIDやオペレーティングシステムプログラムと共にMASK-ROM35に記憶されている。また、HDD2内にも上記MASK-ROM35と同様のMASK-ROMが設けられており、HDD-IDは、このMASK-ROMに記憶されている。このため、リペアセンターでは、デバイスの修理を行った場合には、この修理を行う前に設けられていたMASK-ROMを取り外し、新たなクライアントID或いはHDD-IDが記憶されたMASK-ROMに交換することで、新たなクライアントID或いはHDD-IDの付与を行う。

【 0 1 6 8 】

なお、デバイス自体を新品のデバイスに交換する場合は、この新品のデバイスのMASK-ROM内に、故障したデバイスとは異なるデバイスIDが記憶されているため、上記修理時のようなMASK-ROMの交換は行わない。

【 0 1 6 9 】

次に、リペアセンターのオペレータは、故障したデバイスと共に送付されたメモリカード16のMC-IDを再生する。オペレータは、リペアセンターに設け

られている端末装置を介して上記システムサーバ装置4のデータベース3にアクセスし、上記メモリカード16から再生したMC-IDに基づいて、上記データベース3に記憶されているユーザエントリ情報を参照する。そして、オペレータは、端末装置を操作して、このデータベース3に記憶されているユーザエントリ情報のうち、デバイスIDを、新たに付与したデバイスIDに修正登録する。また、オペレータは、端末装置を介してデータベース3を操作し、コピー済みのコンテンツに対して立てられている上記フラグを降ろす。

【0170】

また、オペレータは、端末装置を操作して、メモリカード16内に記憶されている、MC-Keyで暗号化されたコンテンツジェンキー (Content-Gen-Key) と、コンテンツジェンキー (Content-Gen-Key) で暗号化されたデバイスID (クライアントID及びHDD-ID) とをそれぞれ消去する。そして、このメモリカード16を、修理、交換等したデバイスと共にユーザに返送 (或いは手渡し) する。

【0171】

これにより、ユーザのデバイス (クライアント端末装置1, HDD2及びメモリカード16) の状態は、図5及び図6を用いて説明したユーザ登録行程が終了した直後の状態 (=コンテンツのコピーを行う直前の状態) に戻ることとなる。

【0172】

このメモリカード16とデバイスが返送されたユーザは、図7及び図8を用いて説明したメディアユニークID (MID) の登録とコンテンツキー (Content-Key) の取得を再度行うようにクライアント端末装置1を操作する。

【0173】

クライアント端末装置1は、ユーザの操作に対応してシステムサーバ装置4にアクセスし、メディアユニークID (MID) の登録を行う。そして、クライアント端末装置1は、この登録によりシステムサーバ装置4から取得したコンテンツキー (Content-Key) を用いて光ディスクに記憶されているコンテンツをHDD2に再コピーする。

【0174】

これにより、デバイスの修理や交換によりデバイスIDを新たに付与した場合でも、正規のユーザであれば、新たなデバイスIDに基づいてコンテンツのコピーや再生を実行可能とすることができる。

【0175】

また、コピー管理システム側では、修理や交換により復元したデバイスに対して新たなデバイスIDを付すことにより、修理前のデバイスと修理後のデバイスとを明確に区別して管理することができる。

【0176】

〔メモ리카ードの破損、紛失に対する対応〕

次に、このコピー管理システムの場合、メモ리카ード16の破損、或いは紛失に対しては、以下のように対処する。図14に、このコピー管理システムにおけるメモ리카ード16の破損、紛失に対する対応を説明するための模式図を示す。この図14中、点線の枠で囲んで示すメモ리카ード16が、破損或いは紛失したメモ리카ード16を示している。

【0177】

メモ리카ード16が破損或いは紛失した場合、ユーザは、この図14に示すように、インターネット5を介してクライアント端末装置1をシステムサーバ装置4に接続し、システムサーバ装置4に対してメモ리카ードの再発行を申請する。

【0178】

この申請がなされるとシステムサーバ装置4は、ユーザIDの入力画面データをクライアント端末装置1側に送信する。これにより、ユーザのクライアント端末装置1は、テレビジョン受像機18にユーザIDの入力画面を表示制御する。

【0179】

ユーザは、この入力画面に対してユーザIDの入力を行う。しかし、この場合、メモ리카ード16が破損或いは紛失しているため、メモ리카ード16からユーザID (User ID) を読み出すことはできない。このため、ユーザは、ユーザIDが発行された際にメモ帳等へ書き写しておいたユーザIDを見て、ユーザIDの入力を行う。クライアント端末装置1は、この入力されたユーザIDをシステムサーバ装置4に送信する。

【0180】

次にシステムサーバ装置4は、このユーザから送信されたユーザIDに対応するユーザエントリ情報をデータベース3から参照する。これにより、システムサーバ装置4は、破損或いは紛失したメモ리카ード16のMC-ID及びMC-Keyと共に、コンテンツジェンキー (Content-Gen-Key) やそのメモ리카ード16でコピーされたコンテンツ等を認識することができる。

【0181】

次に、システムサーバ装置4は、新たなMC-IDを有するメモ리카ード16 newに対して、新たなMC-Key (New-MC-Key) と、このNew-MC-Keyで新たに暗号化したコンテンツジェンキー (Content-Gen-Key) と、このコンテンツジェンキー (Content-Gen-Key) で暗号化したクライアントID及びHDD-IDを記録し直す。

また、システムサーバ装置4は、データベース3に記憶されているユーザエントリ情報が、この新たなメモ리카ード16 Newに対応したユーザエントリ情報となるように、MC-IDやMC-Key等の書き換えを行う。

【0182】

なお、この場合、メモ리카ード16が破損或いは紛失した場合であり、ユーザのクライアント端末装置1及びHDD2は正常に動作している。このため、コンテンツジェンキー (Content-Gen-Key) で暗号化されるクライアントID及びHDD-IDとしては、元のデバイスIDがそのまま用いられる。

【0183】

次に、リペアセンターは、このメモ리카ード16 newを、例えば郵送等によりユーザ側に物理的に送付する。前述のように、システムサーバ装置4側ではこのメモ리카ード16 new内の各情報の書き換えと共に、データベース3のユーザエントリ情報の書き換えを行っている。このため、送付されたメモ리카ード16 newを受け取ったユーザは、このメモ리카ード16 new、クライアント端末装置1及びHDD2の組み合わせのシステムを用いて、以前と同様に、コンテンツのコピーや、コピーしたコンテンツの再生等を行うことができる。

【0184】

〔第 1 の実施の形態の効果〕

以上の説明から明らかなように、この第 1 の実施の形態のコピー管理システムは、システム管理者が、コンテンツキーで暗号化処理を施したコンテンツを、メディアユニーク I D (M I D) が付された光ディスクに記憶させてユーザに配布する。

【 0 1 8 5 】

ユーザは、コンテンツのコピーを行う際に、システムサーバ装置 4 に対して光ディスクの M I D を送信する。また、ユーザは、自分が使用しているデバイスのデバイス I D (クライアント I D, H D D - I D, M C - I D 等) をシステムサーバ装置 4 に送信する。

【 0 1 8 6 】

システムサーバ装置 4 は、各ユーザが使用しているデバイスのデバイス I D に関連付けて、過去にコンテンツのコピーが行われた光ディスクの M I D をデータベース 3 に記憶している。

【 0 1 8 7 】

システムサーバ装置 4 は、ユーザからコンテンツのコピー申請がなされた際に、ユーザが使用しているデバイス I D と光ディスクの M I D 基づいてデータベース 3 を参照する。システムサーバ装置 4 は、データベース 3 内に同じ M I D が登録されていないことを条件として、コンテンツを復号化するためのコンテンツキーを、ユーザのクライアント端末装置 1 に送信する。

【 0 1 8 8 】

クライアント端末装置 1 は、このコンテンツキーを用いて光ディスクに記憶されているコンテンツを復号化して H D D 2 にコピーする。

【 0 1 8 9 】

このコピー管理システムは、データベース 3 内に登録されている M I D と同じ M I D を掲示してコピー申請がなされた場合は、上記コンテンツキーの配信は行われぬ。このため、このコピー管理システムは、コンテンツのコピーを 1 回に制限することができ、コンテンツの不正コピーを防止することができる。

【 0 1 9 0 】

〔第 2 の実施の形態〕

次に本発明の第 2 の実施の形態となるコピー管理システムの説明をする。上述の第 1 の実施の形態のコピー管理システムは、ユーザが自分のクライアント端末装置 1 をシステム管理者側のシステムサーバ装置 4 に直接的に接続してユーザ登録を行い、コンテンツキー (Content-Key) 等を取得してコンテンツのコピーを行うものであった。

【0191】

この第 2 の実施の形態のコピー管理システムは、ユーザのクライアント端末装置 1 とシステム管理者側のシステムサーバ装置 4 との間に、第 3 者が管理する第 3 者管理サーバ装置が設けられている。ユーザはこの第 3 者管理サーバ装置を介してコンテンツキー (Content-Key) 等の取得を行う。第 3 者管理サーバ装置は、このコンテンツキー (Content-Key) 等の提供に対する課金を行う。

【0192】

〔第 2 の実施の形態の構成〕

図 15 に、この第 2 の実施の形態となるコピー管理システムのシステム構成図を示す。この図 15 は、光ディスクからコンテンツをコピーする際にコンテンツキー (Content-Key) を取得する流れを示している。

【0193】

この図 15 において、システムサーバ装置 4 と第 3 者管理サーバ装置 50 とは、例えば専用回線や、公衆回線を専用回線のように利用可能な VPN (Virtual Private Network) 等により相互に接続されている。

【0194】

また、システムサーバ装置 4 はインターネット 5 には接続されておらず、この第 3 者管理サーバ装置 50 がインターネット 5 に接続されている。このため、ユーザは、システムサーバ装置 4 に対して直接的にアクセスすることはできず、この第 3 者管理サーバ装置 50 を介して間接的にシステムサーバ装置 4 にアクセスすることとなる。

【0195】

〔第 2 の実施の形態の動作〕

次に、この第 2 の実施の形態のコピー管理システムの動作説明をする。この第 2 の実施の形態のコピー管理システムの場合、光ディスクからコンテンツのコピーを行おうとするユーザは、インターネット 5 を介して自分のクライアント端末装置 1 を第 3 者管理サーバ装置 5 0 に接続する。そして、ユーザは、クライアント端末装置 1 を介して、MC-ID, ユーザ ID (User ID), メディアユニーク ID (MID) を第 3 者管理サーバ装置 5 0 側に送信する。また、ユーザは、クライアント端末装置 1 を介して、第 3 者管理サーバ装置 5 0 用のアカウント情報（例えばユーザ名やパスワード等）を第 3 者管理サーバ装置 5 0 に送信する。

【0196】

クライアント端末装置 1 は、MC-ID 及びアカウント情報をそのまま第 3 者管理サーバ装置 5 0 に送信する。また、クライアント端末装置 1 は、ユーザ ID (User ID) 及び光ディスクのメディアユニーク ID (MID) を MC-Key で暗号化し、これらを第 3 者管理サーバ装置 5 0 に送信する。

【0197】

第 3 者管理サーバ装置 5 0 は、クライアント端末装置 1 から送信された各情報のうち、アカウント情報を抽出して取得する。また、第 3 者管理サーバ装置 5 0 は、専用回線（或いは上記 VPN）を介して MC-ID, MC-Key で暗号化されたユーザ ID (User ID)、及び MC-Key で暗号化されたメディアユニーク ID (MID) をシステムサーバ装置 4 に送信する。

【0198】

システムサーバ装置 4 は、この MC-ID, ユーザ ID 及び MID を受信すると、前述と同様に暗号化されて光ディスクに記録されているコンテンツを復号化するためのコンテンツキー (Content-Key) を MC-Key で暗号化して第 3 者管理サーバ装置 5 0 に返信する。また、システムサーバ装置 4 は、コンテンツジェンキー (Content-Gen-Key) を MC-Key で暗号化して第 3 者管理サーバ装置 5 0 に返信する。さらにシステムサーバ装置 4 は、このコンテンツジェンキー (Content-Gen-Key) でユーザのクラ

クライアントID及びHDD-IDを暗号化して第3者管理サーバ装置50に返信する。

【0199】

第3者管理サーバ装置50は、このMC-Keyで暗号化されたコンテンツキー（Content-Key）、MC-Keyで暗号化されたコンテンツジェンキー（Content-Gen-Key）、及びコンテンツジェンキー（Content-Gen-Key）で暗号化されたユーザのクライアントID、HDD-IDを、それぞれインターネット5を介してユーザのクライアント端末装置1に転送する。

【0200】

第3者管理サーバ装置50は、コンテンツキー（Content-Key）を提供した代償として、先にクライアント端末装置1から送信された第3者管理サーバ装置50用のアカウント情報に基づいて、そのユーザに対する課金を行う。

【0201】

クライアント端末装置1は、第3者管理サーバ装置50から送信された上記コンテンツキー、コンテンツジェンキー、クライアントID、及びHDD-IDをメモリカード16に記憶制御して、前述のようにコンテンツのコピー、及びコピーしたコンテンツの再生に用いる。

【0202】

第3者管理サーバ装置50側には、例えばユーザのクレジットカードの番号や、プリペイドされた金額情報が予め登録されている。このため、第3者管理サーバ装置50は、コンテンツキーの提供と引き替えに課金した金額をクレジットカード会社に請求して回収する。或いは第3者管理サーバ装置50は、プリペイドされている残金から課金分の金額を減算して回収する。

【0203】

このように回収された金銭は、例えばシステムサーバ装置4の管理者と第3者管理サーバ装置50の管理者との間において、所定の割合で分配されることとなる。

【0204】

〔第 2 の実施の形態の効果〕

このようにこの第 2 の実施の形態のコピー管理システムは、クライアント端末装置 1 とシステムサーバ装置 4 との間に第 3 者管理サーバ装置 5 0 を設けて構成する。ユーザはこの第 3 者管理サーバ装置 5 0 を介してシステムサーバ装置 4 にアクセスしてコンテンツキー (Content-Key) の配布を請求する。第 3 者管理サーバ装置 5 0 は、このコンテンツキー (Content-Key) をユーザに配布して課金を行う。

【0205】

これにより、このコピー管理システムは、第 3 者 (第 3 者管理サーバ装置 5 0 の管理者) が介在するコピー管理システムという新規なコピー管理システムを提供することができる他、上述の第 1 の実施の形態のコピー管理システムと同じ効果を得ることができる。

【0206】

また、このコピー管理システムは、コンテンツキーをユーザに配布した際に課金を行うことで、光ディスク等を介して、或いは所定のネットワークを介してコンテンツを無償でユーザに配布することができる。

【0207】

なお、このコピー管理システムにおいて、光ディスクに M I D を付すことなくユーザに配布し、ユーザからコピーの申請があった際に、システムサーバ装置 4 或いは第 3 者管理サーバ装置 5 0 が、そのユーザに対してコンテンツキーを配布して課金を行うようにしてもよい。

【0208】

また、この第 2 の実施の形態のコピー管理システムは、第 3 者管理サーバ装置 5 0 が課金を行うこととしたが、これは、システムサーバ装置 4 が課金を行うようにしてもよい。

【0209】

最後に、本発明は一例として説明した上述の各実施の形態に限定されることはない。このため、上述の各実施の形態以外であっても、本発明に係る技術的思想を逸脱しない範囲であれば、設計等に応じて種々の変更が可能であることは勿論

である。

【0210】

例えば、上述の各実施の形態の説明では、クライアント端末装置1は、デバイス識別情報として、クライアントID、HDD-ID及びMC-IDをシステムサーバ装置4に送信することとした。しかし、クライアント端末装置1からクライアントIDのみをシステムサーバ装置4に送信してもよい。同様に、クライアント端末装置1からHDD-IDのみをシステムサーバ装置4に送信してもよい。同様に、クライアント端末装置1からMC-IDのみをシステムサーバ装置4に送信してもよい。

【0211】

また、クライアント端末装置1からクライアントID及びHDD-IDをシステムサーバ装置4に送信してもよい。同様に、クライアント端末装置1からクライアントID及びMC-IDをシステムサーバ装置4に送信してもよい。同様に、クライアント端末装置1からHDD-ID及びMC-IDをシステムサーバ装置4に送信してもよい。

【0212】

すなわち、上述の各実施の形態のコピー管理システムは、システムサーバ装置4側で、コンテンツのコピーが行われる記憶媒体と、コンテンツのコピーに使用されるデバイスとを関連付けてコピー管理を行うことで不正コピーを防止する。このため、クライアント端末装置1からシステムサーバ装置4に送信されるデバイス識別情報としては、ユーザを特定可能な識別情報であればよい。

【0213】

また、上述の各実施の形態の説明では、メモリカード16を用いることとしたが、このコピー管理システムの場合、必ずしもメモリカード16は必要としない。メモリカード16を用いない場合は、メモリカード16に記憶される上記コンテンツキーやコンテンツジェンキー等は、HDD2やクライアント端末装置1に内蔵されているメモリに記憶させればよい。

【0214】

【発明の効果】

本発明は、記憶媒体の持ち主である正規のユーザに対してのみ、記憶媒体に記憶されたコンテンツのコピーを許可することができる。このため、記憶媒体に記憶されたコンテンツの不正コピーを防止することができる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施の形態のコピー管理システムのシステム構成を示すブロック図である。

【図 2】

コピー管理システムを構成するクライアント端末装置及びハードディスクドライブ（HDD）の外観を示す斜視図である。

【図 3】

クライアント端末装置の電氣的な構成を示すブロック図である。

【図 4】

コンテンツキー（Content-Key）で暗号化されたデジタルコンテンツが記憶された、このコピー管理システムに用いられる光ディスクを説明するための図である。

【図 5】

コピー管理システムにおけるユーザ登録の流れを示すフローチャートである。

【図 6】

ユーザ登録時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示すコピー管理システムの模式図である。

【図 7】

コピー管理システムにおける、光ディスクに個別に付されたメディアユニーク ID（MID）の登録動作と、コンテンツキー（Content-Key）の取得動作を示すフローチャートである。

【図 8】

光ディスクに個別に付されたメディアユニーク ID（MID）の登録時、及びコンテンツキー（Content-Key）の取得時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示すコピー管理システムの模

式図である。

【図 9】

コピー管理システムにおけるコピー行程の流れを示すフローチャートである。

【図 1 0】

コピー実行時にクライアント端末装置、メモリカード及びハードディスクドライブの間で送受信される各情報を示す模式図である。

【図 1 1】

コピー管理システムにおける、ハードディスクドライブにコピーしたデジタルコンテンツの再生動作を示すフローチャートである。

【図 1 2】

ハードディスクドライブにコピーしたデジタルコンテンツの再生時に、クライアント端末装置、メモリカード及びハードディスクドライブの間で送受信される情報を示す模式図である。

【図 1 3】

クライアント端末装置或いはハードディスクドライブの修理或いは交換に対するコピー管理システムの対応を説明するための模式図である。

【図 1 4】

メモリカードの破損或いは紛失に対するコピー管理システムの対応を説明するための模式図である。

【図 1 5】

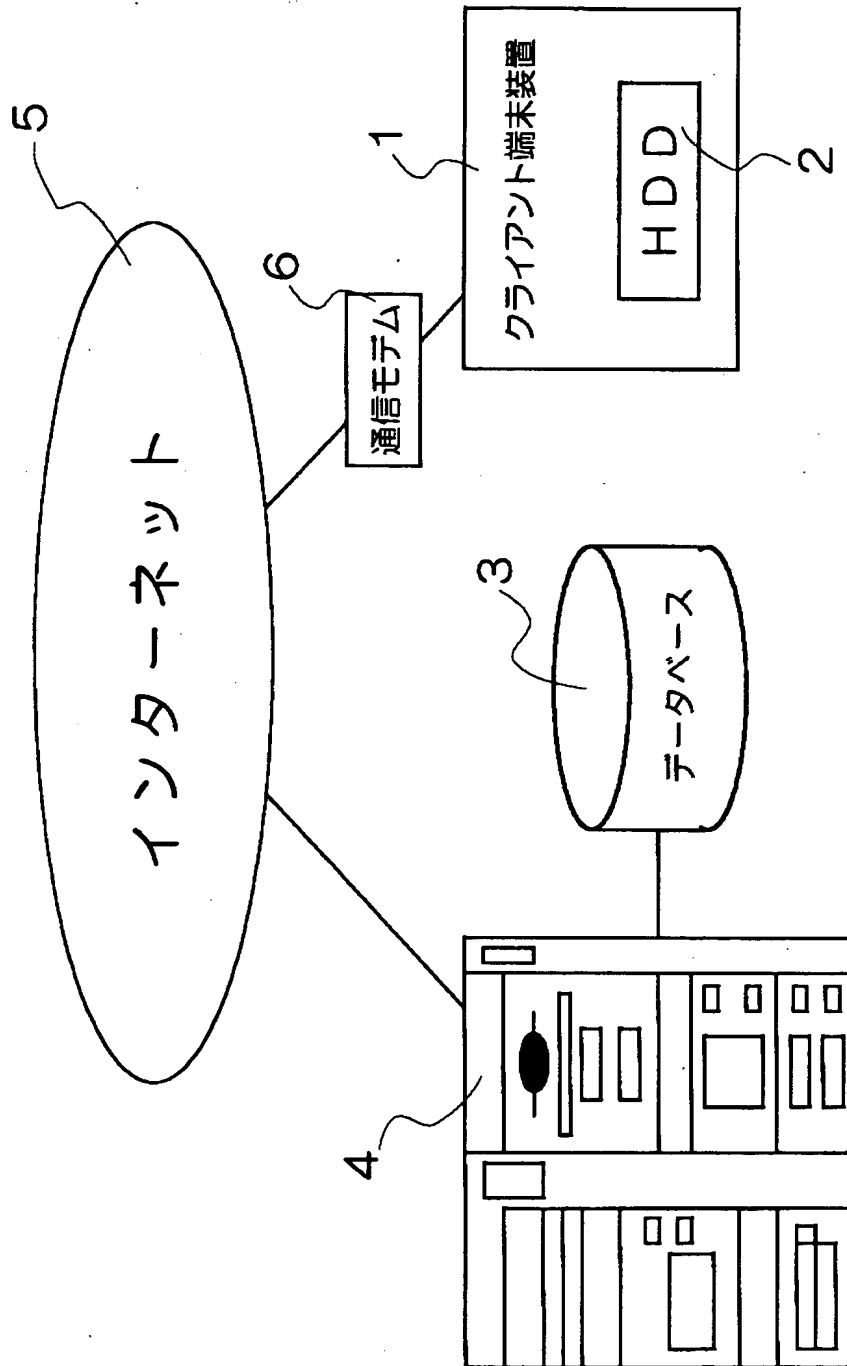
光ディスクに個別に付されたメディアユニーク ID (M I D) の登録時、及びコンテンツキー (C o n t e n t - K e y) の取得時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示す、本発明の第 2 の実施の形態となるコピー管理システムの模式図である。

【符号の説明】

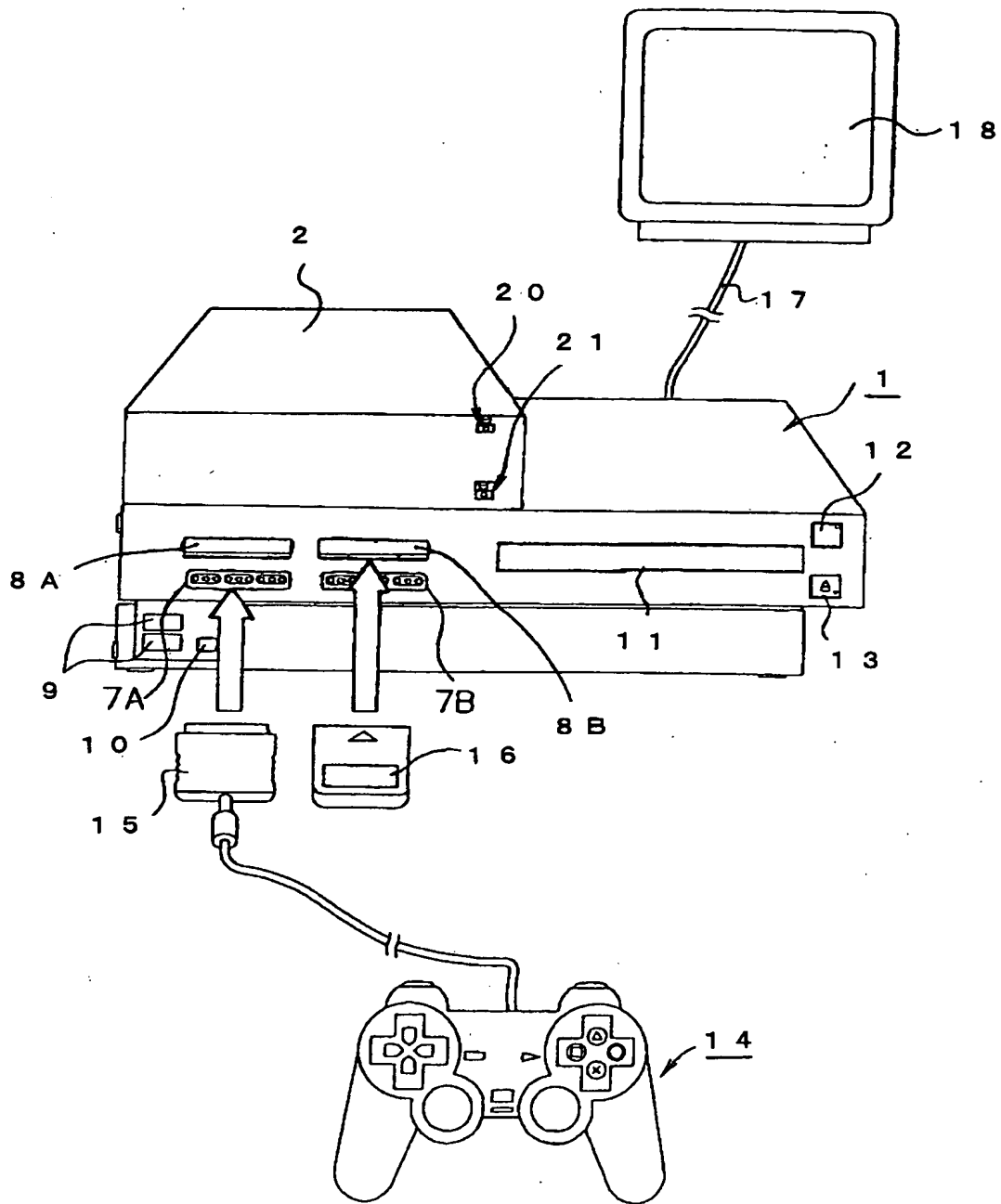
1 …クライアント端末装置、 2 …ハードディスクドライブ (HDD), 3 …データベース, 4 …システムサーバ装置, 5 …インターネット, 6 …通信モデム

【書類名】 図面

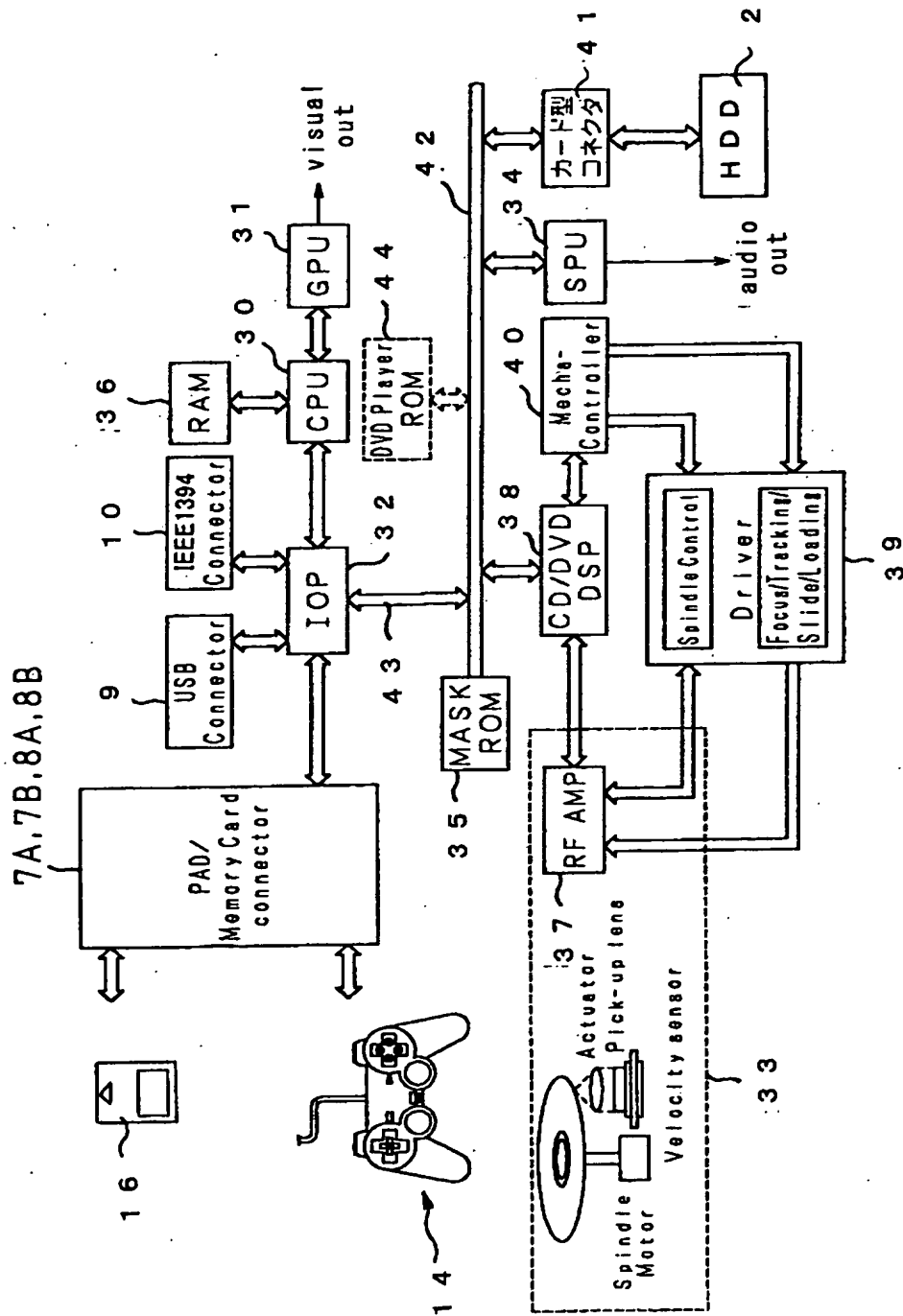
【図1】



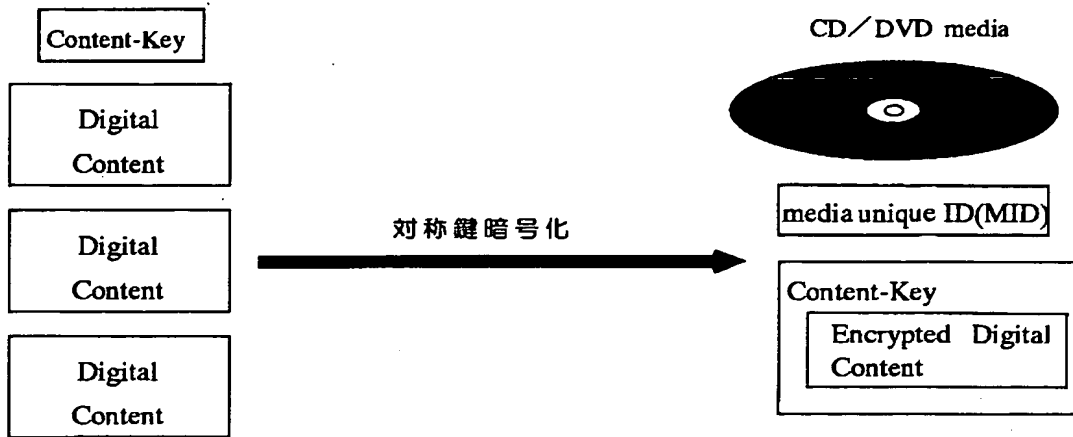
【図 2】



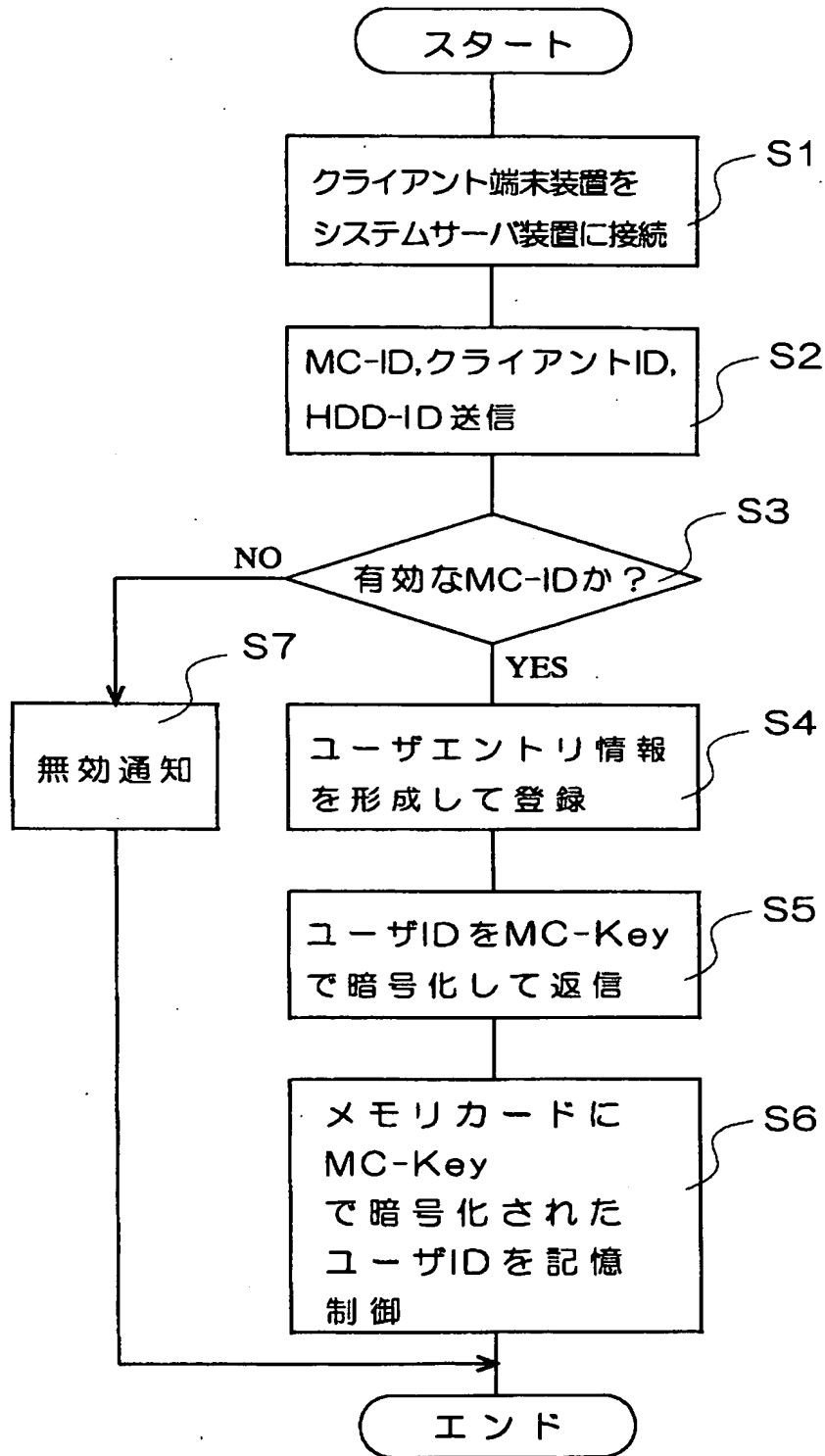
【図 3】



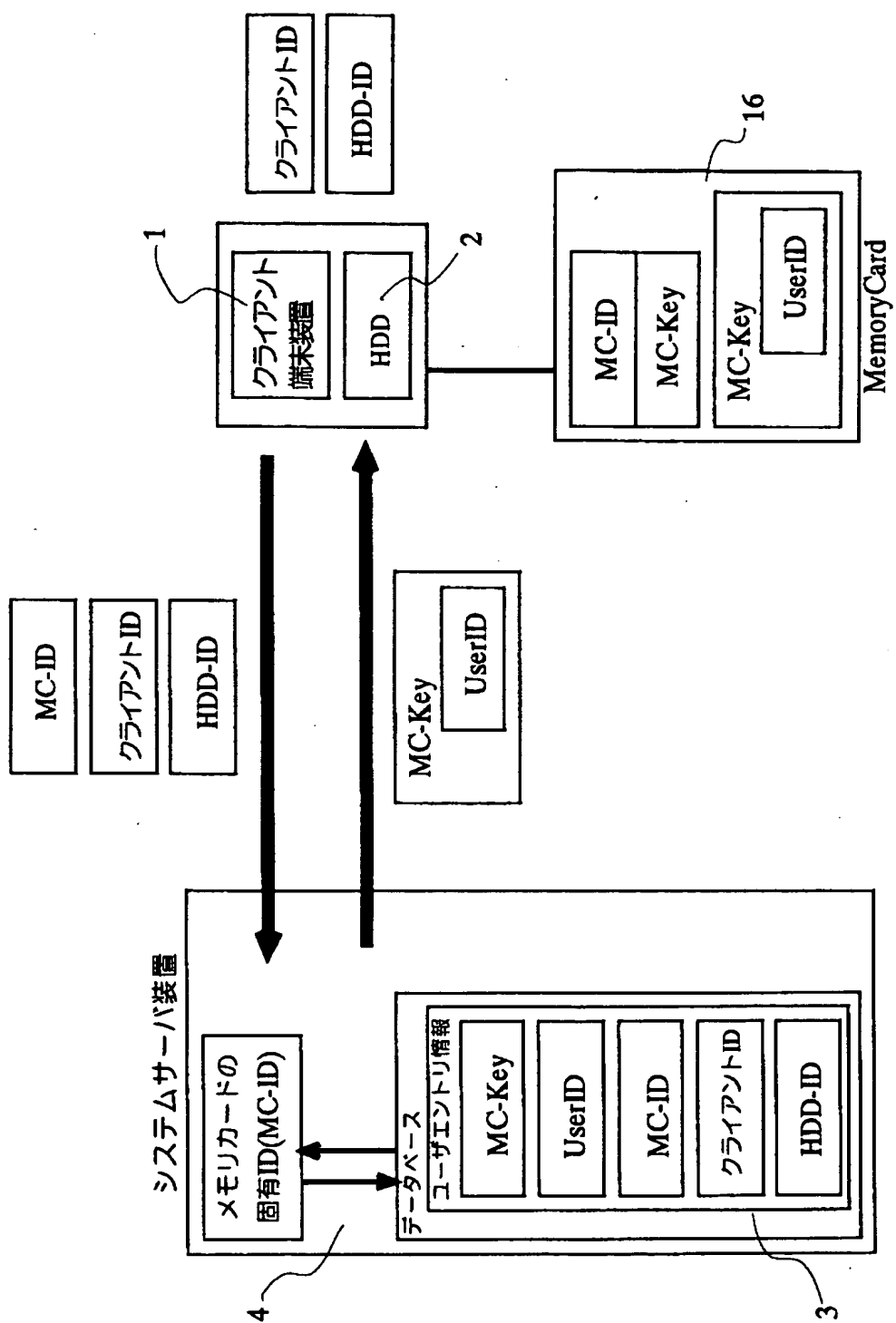
【図 4】



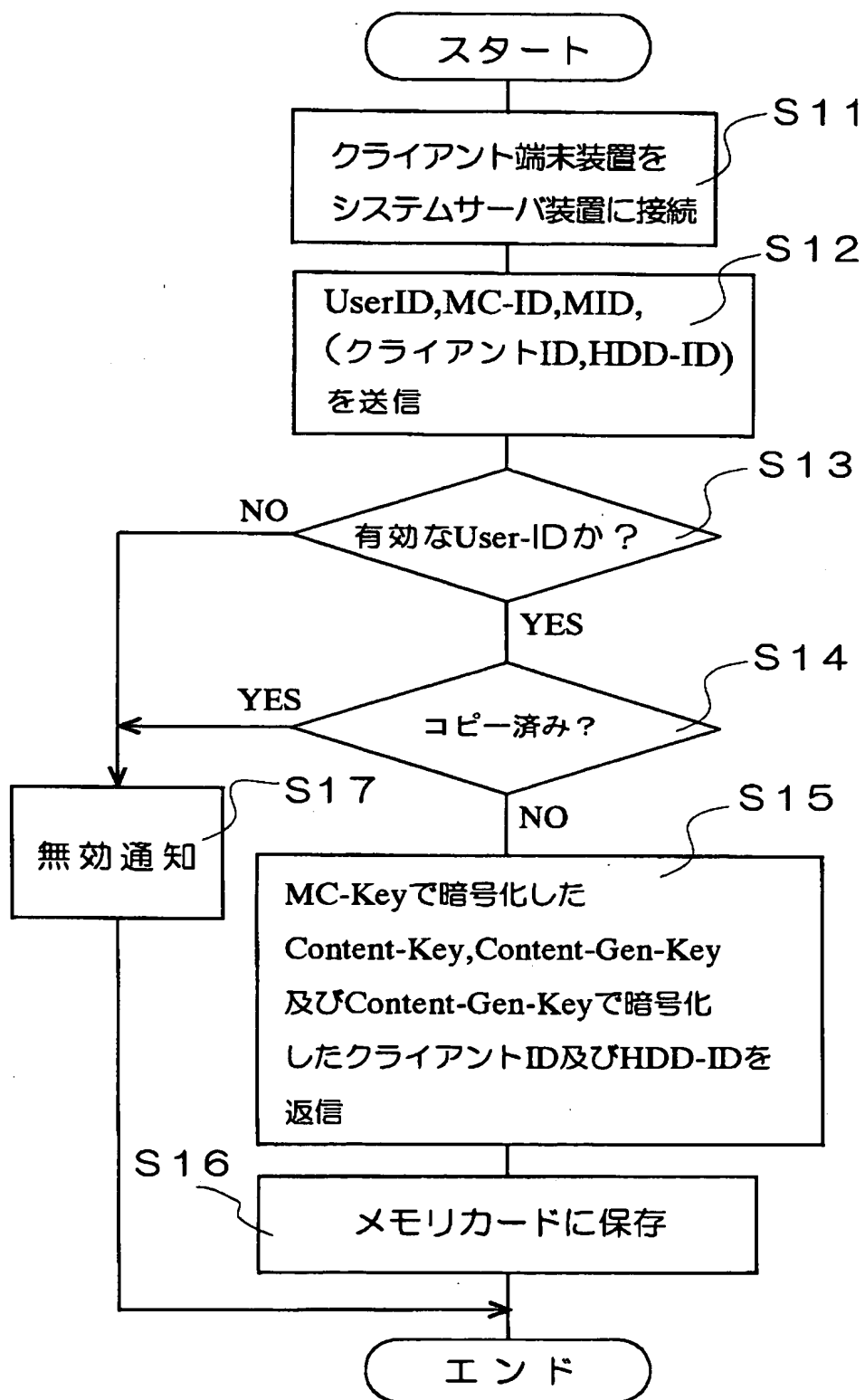
【図 5】



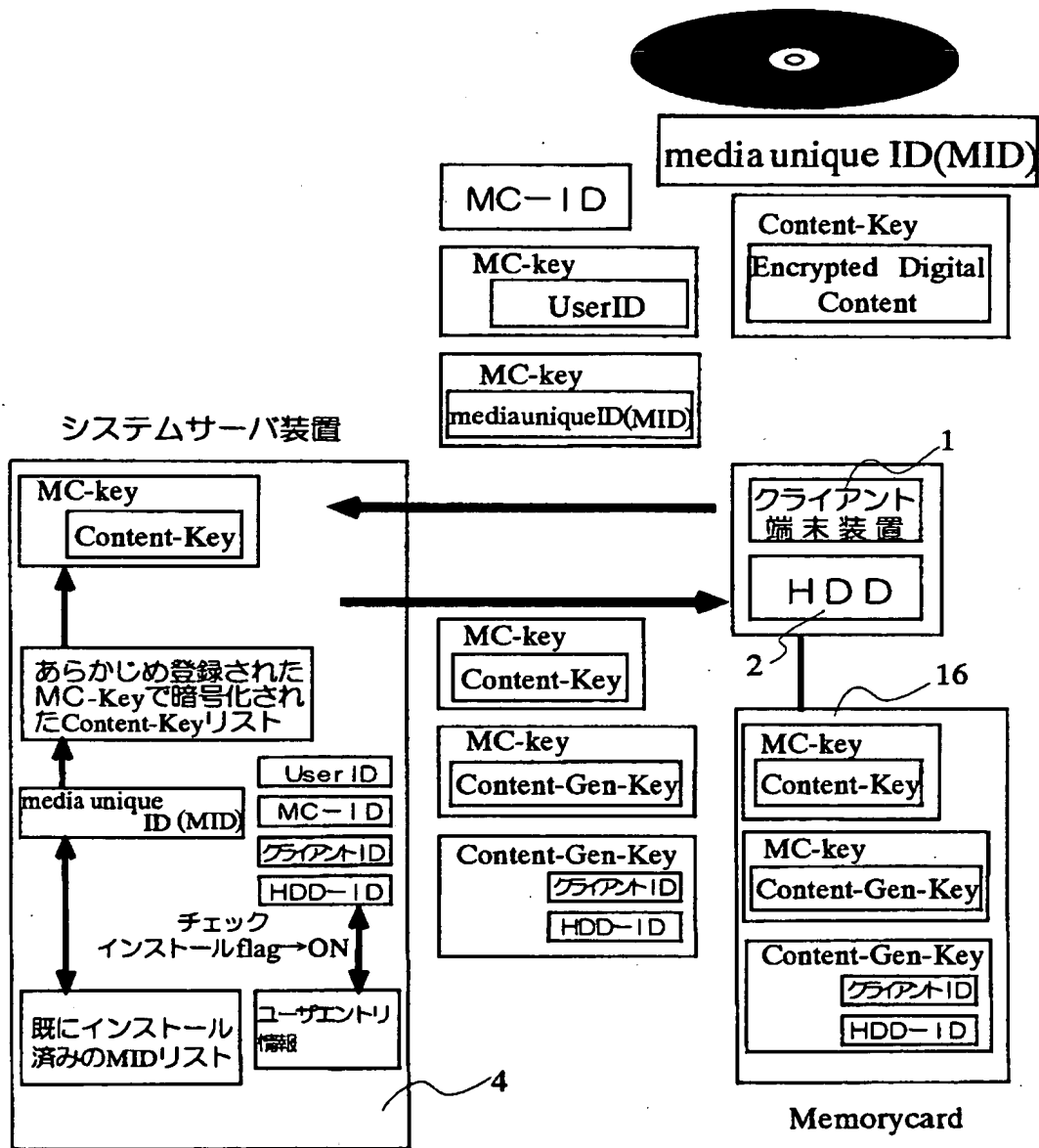
【图 6】



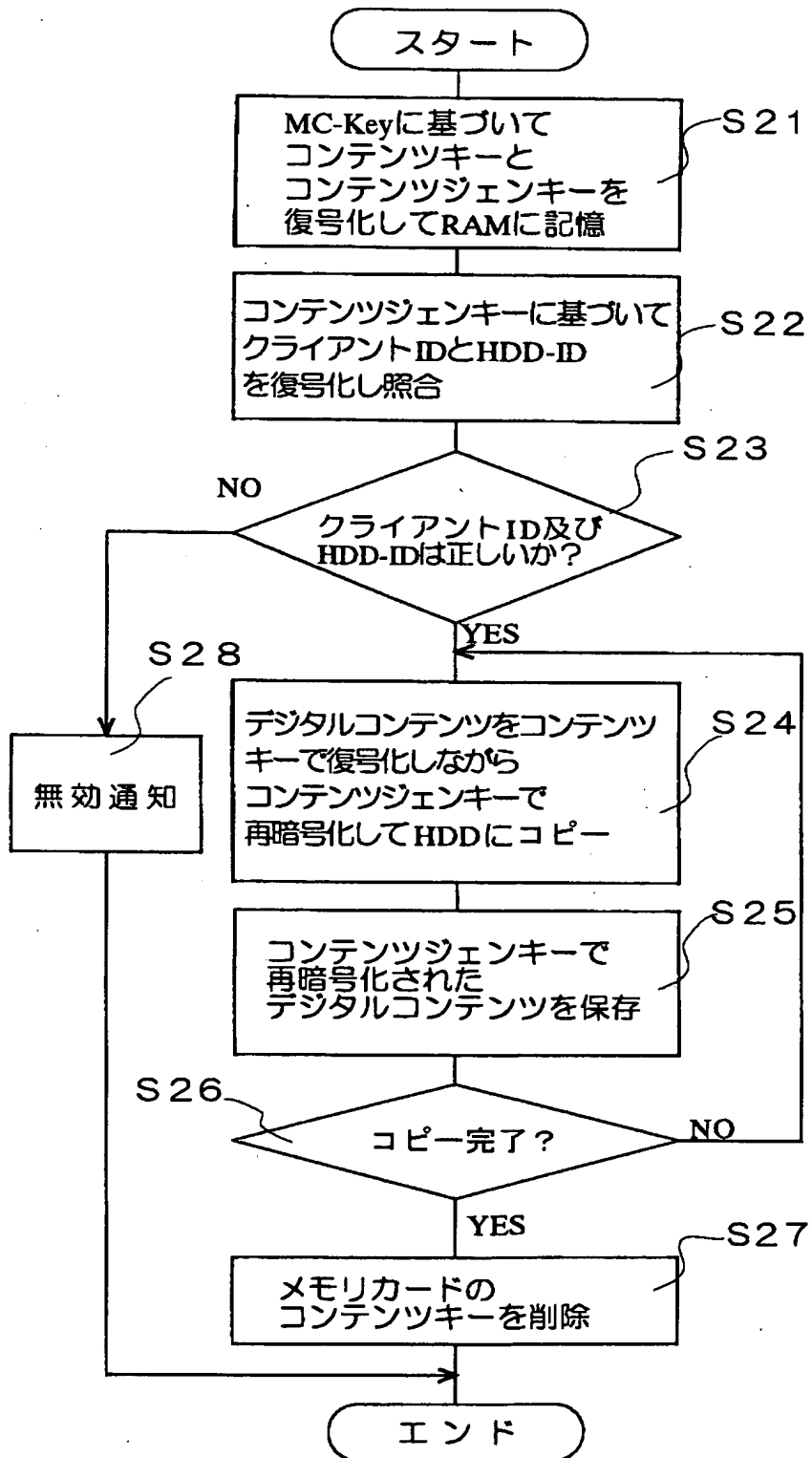
【図 7】



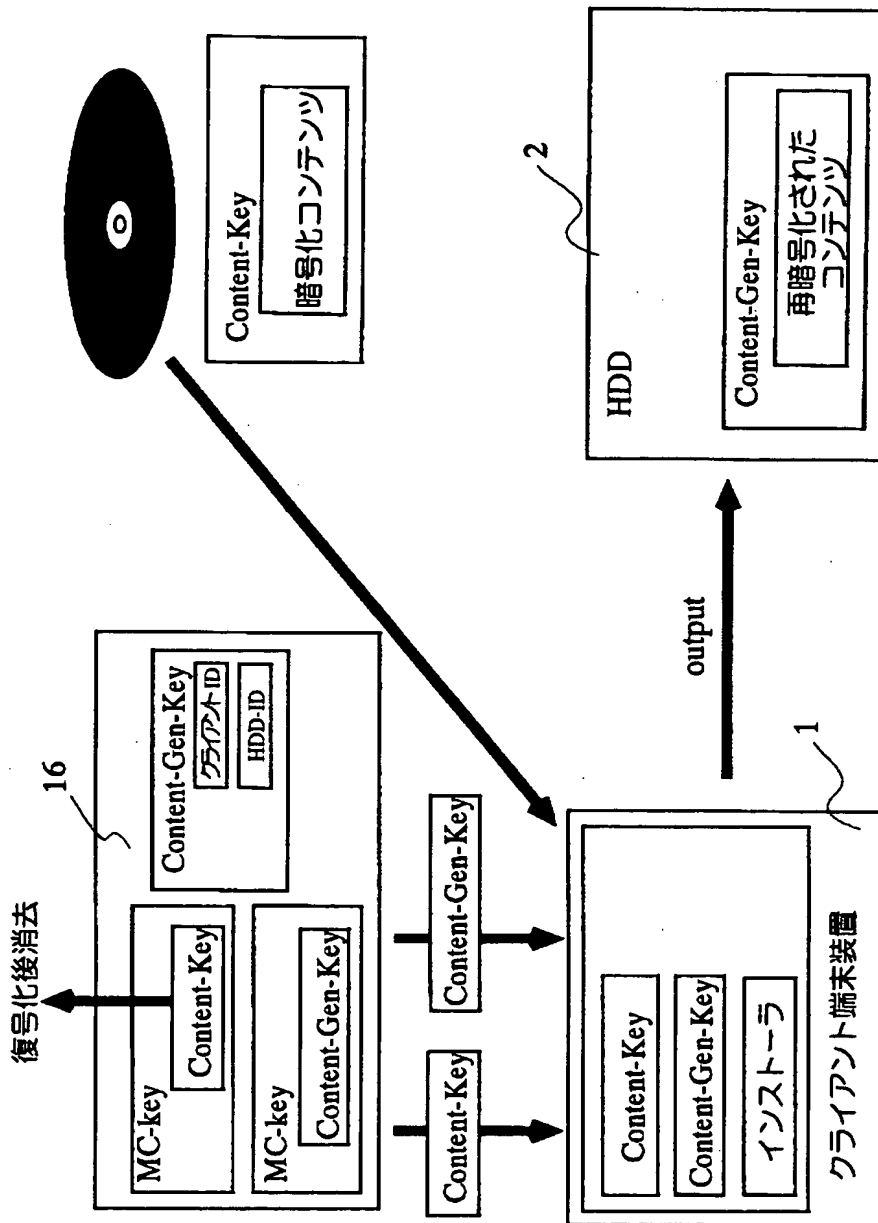
【図 8】



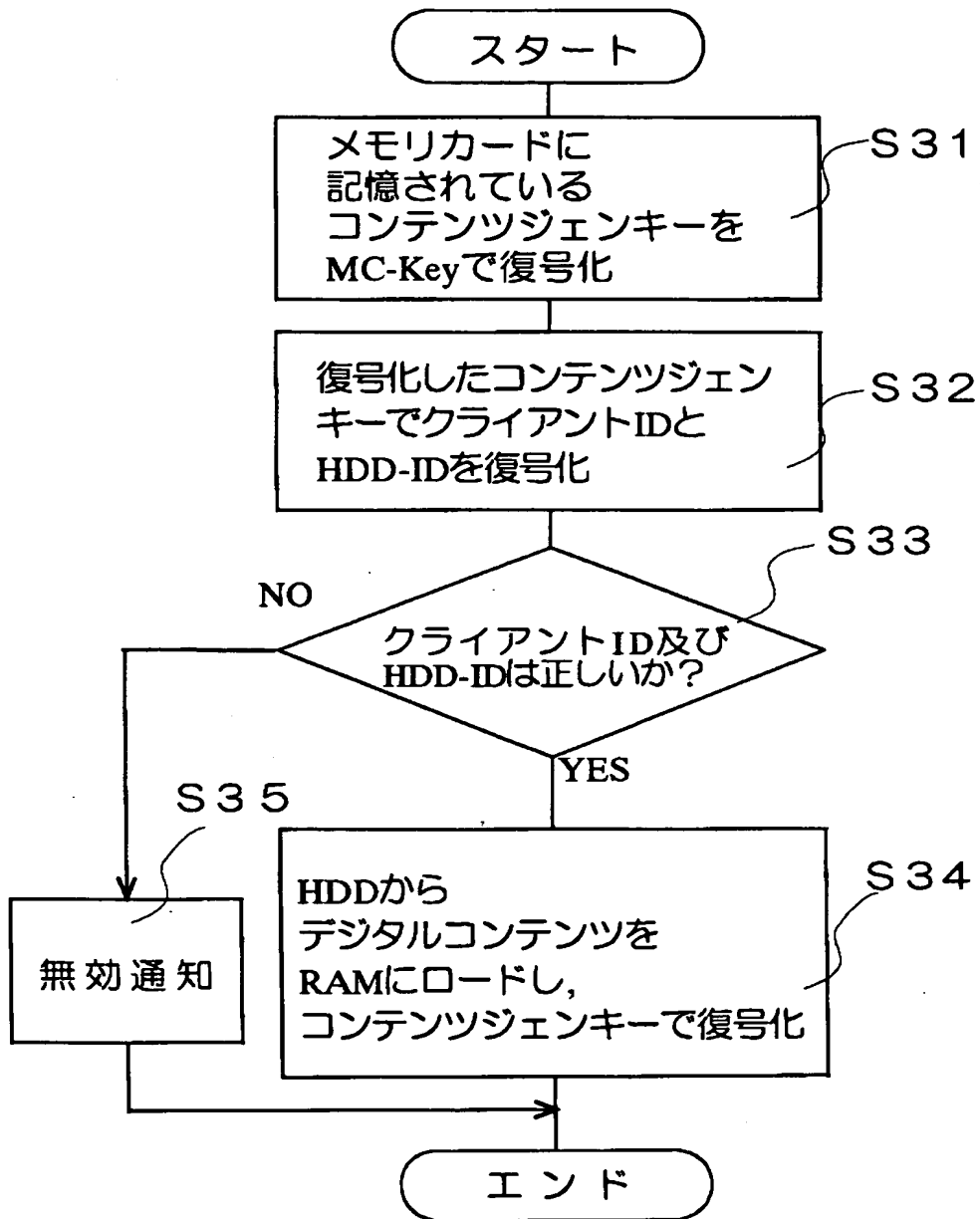
【図 9】



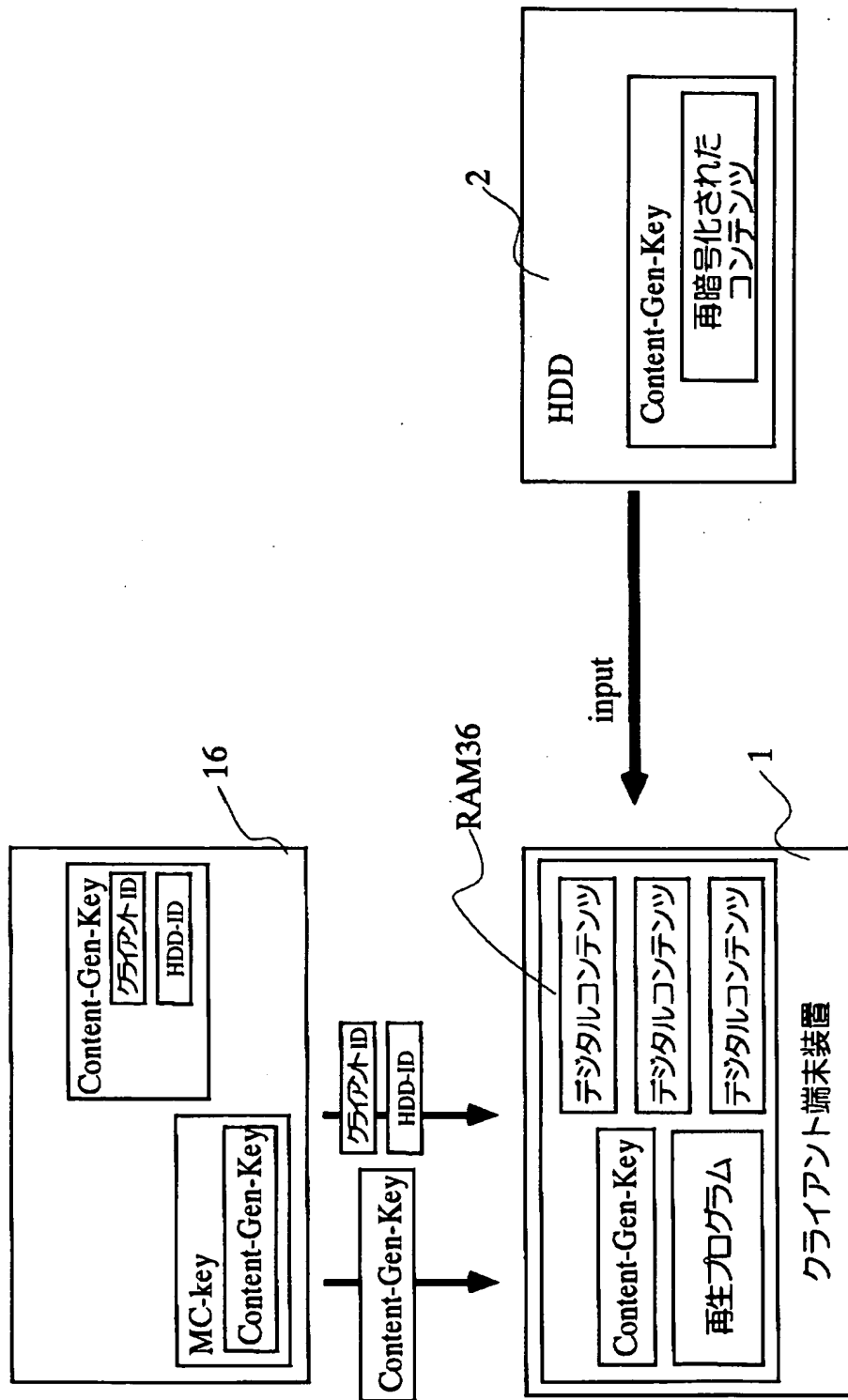
【図 10】



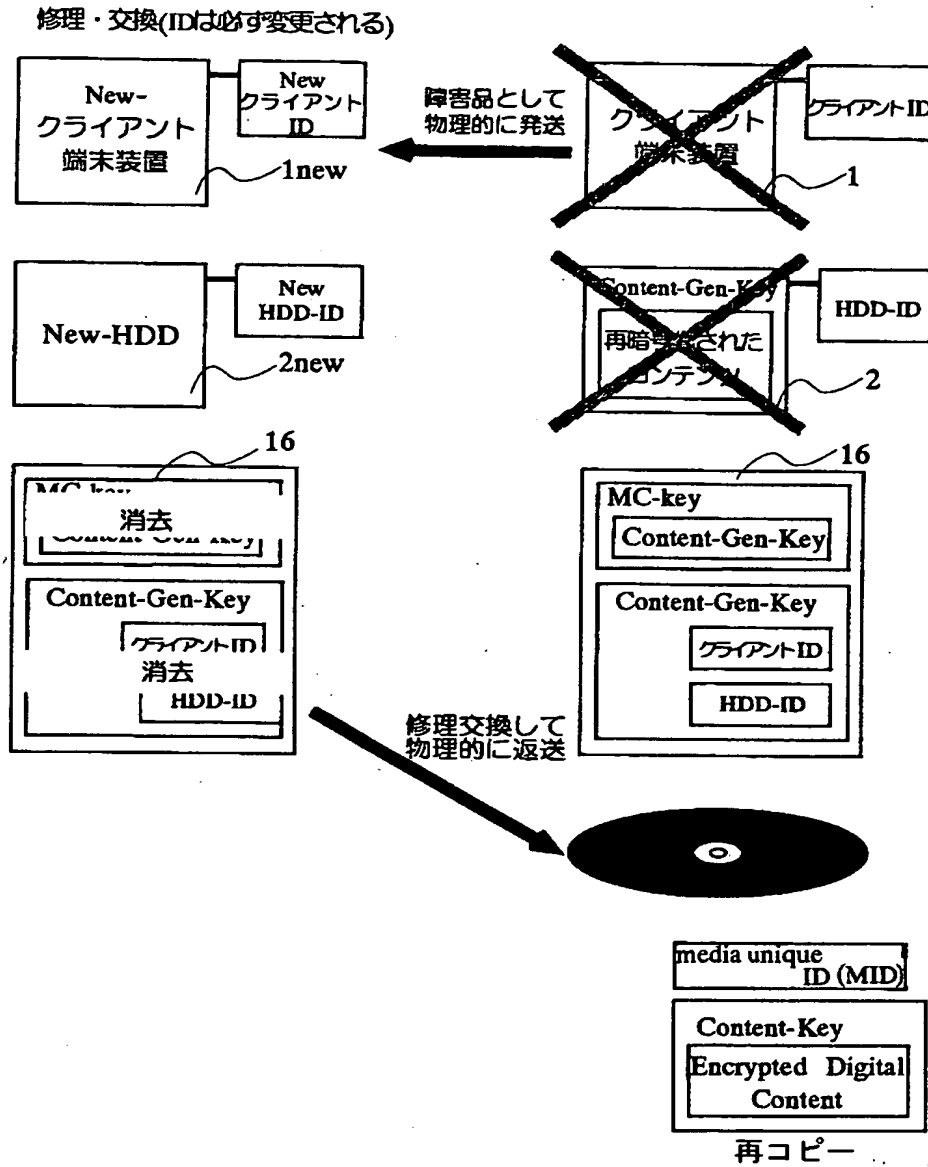
【図 11】



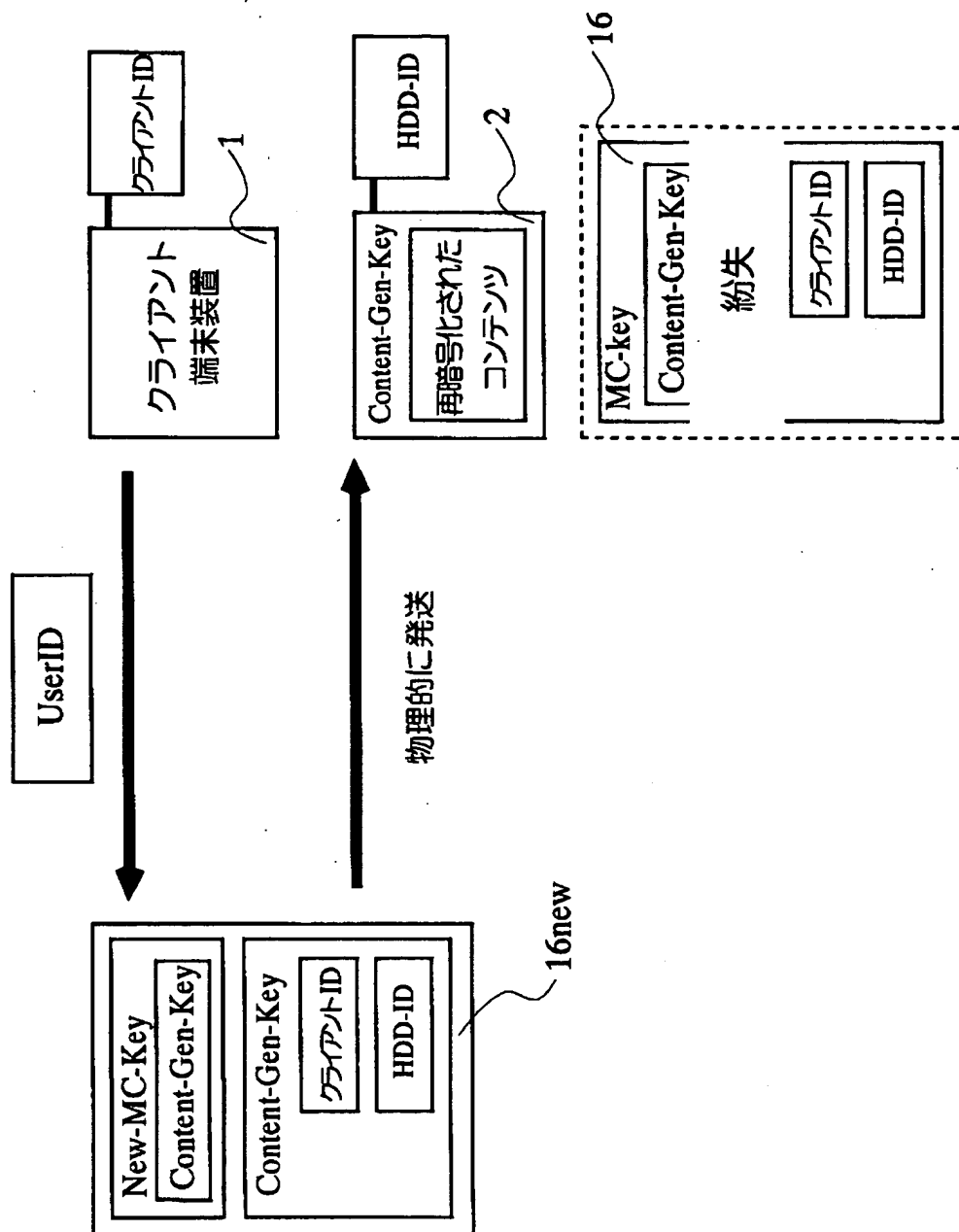
【図 12】



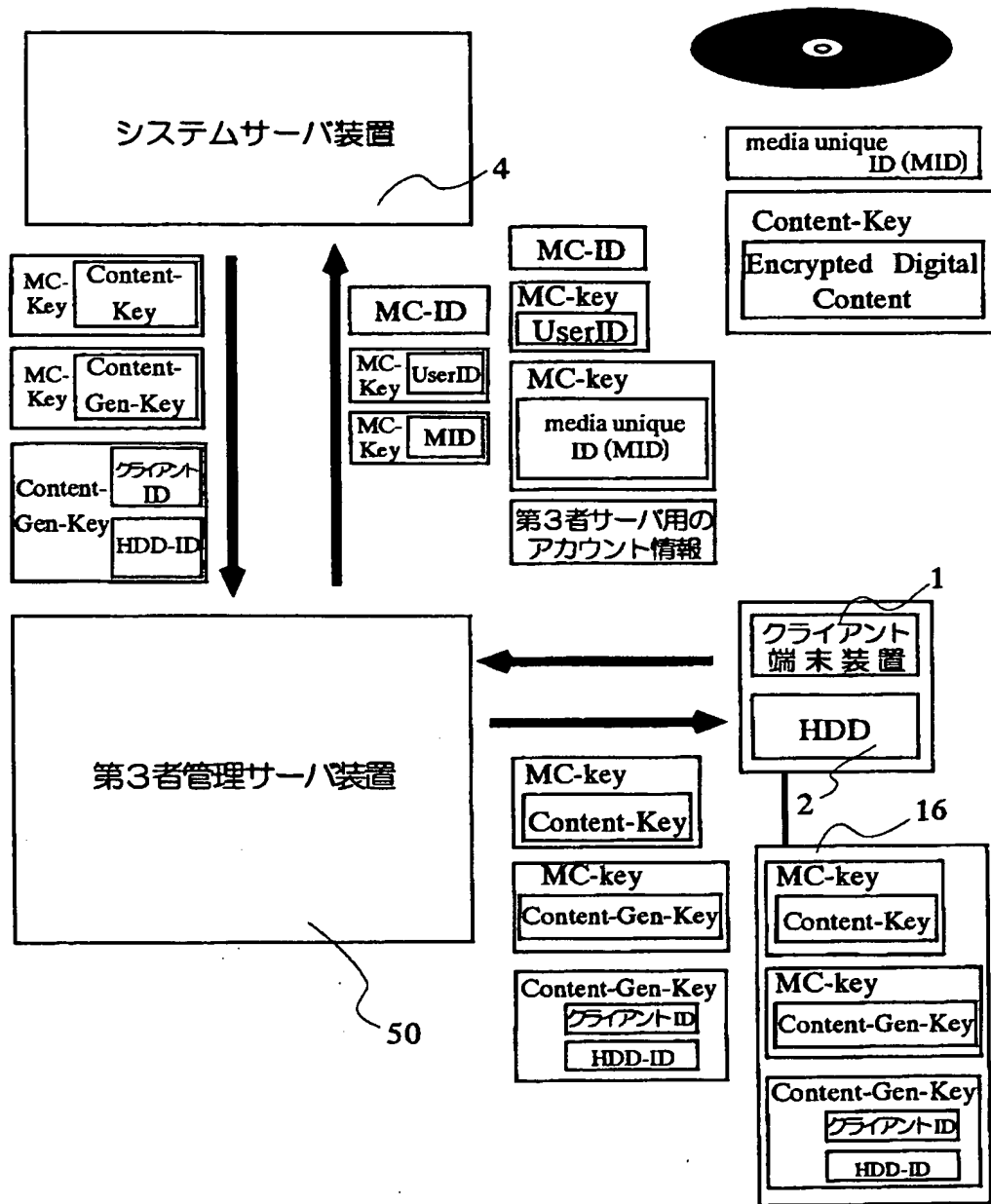
【図 13】



【図 14】



【図 15】



【書類名】 要約書

【要約】

【課題】 コンテンツの不正コピーを防止する。

【解決手段】 各光ディスク毎に I D (MID) を付すと共に、コンテンツをContent-Keyで暗号化して記録しておく。システムサーバ装置は、ユーザが所有するクライアント端末装置のクライアント I D, H D D のHDD-ID、及びメモ리카ードのMC-ID等をユーザエントリ情報として管理する。ユーザはコンテンツのコピーを行う際に、光ディスクのMIDと共にMC-IDをシステムサーバ装置に送信する。システムサーバ装置は、MC-IDをユーザエントリ情報と照合してユーザを特定し、コンテンツの暗号化の際に用いたContent-Keyを返送する。ユーザ側では、この返送されたContent-Keyを用いて光ディスクに記録されているコンテンツを復号化しHDDにコピーする。記憶媒体の持ち主である正規のユーザにのみ、コンテンツのコピーが許可されるため、コンテンツの不正コピーを防止することができる。

【選択図】 図 8

出 願 人 履 歴 情 報

識別番号 [395015319]

1. 変更年月日 1997年 3月31日

[変更理由] 住所変更

住 所 東京都港区赤坂7-1-1

氏 名 株式会社ソニー・コンピュータエンタテインメント